Edition: 99/12

Language: English

Reference: ECI25020.DOC

Authors: DB, FA, GJ, GM

IP Network connectivity
Ethernet - TCP/IP
Integrated services:
HTTP (web), TELNET (console), FTP (file),
SMTP (mail), SNMP (agent, proxy)
Filing system
Events and history log manager

IP2
System

REFERENCE MANUAL

V1.4

CONTENTS

Changes 1.0 to 1.1

Introduction of "VIEW" commands.

USERS? command replaced by VIEW.USERS

NETWORK? command replaced by VIEW.NETWORK

VER command replaced by VER?

Command and security in telnet: SECURE=ON / OFF

Network technical glossary

Do not forget to display the lower part of the MAC address for SN?

See the VIEW commands and implant them, in particular VIEW.SYSTEM

Addition of Web Counter

Form: action= no longer contains CGI.EXE but the name of the page to be returned

Changes 1.1 to 1.2

Editorial modifications between VIEW.USERS? and VIEW.USERS, deletion of VIEW.USER

The CLEAR_WEB_CNT command replaced by WEB_CNT=x.

The WEB_CNT counter is not reset to zero on each RESET.

Command execution by an html link: the name of the page is no longer CGI.EXE but the name of the page to be returned after executing the command.

Changes 1.2 to 1.3

1.3: same as V1.4 beta. See 1.4.

Changes 1.3 to 1.4

Editorial modifications between ?USERS

Replacement of the VIEW.<objet> syntax by ?<objet>

SNMP management specified: generic trap **IP2_TRAP**

SNMP: specification of MIBs supported as standard

EVENTS:

- properties
- associated generation of trap, email, sending a file etc…

SECURE_CGI parameter added to allow CGI actions to be protected independently of the access to the web pages: this measure can be used to add an http client level and leads to:

- public http (web) client (pages in directory /html, free access)
- private with password (pages in directory /, access can be protected by SECURE=ON)
- CGI authorised (CGI actions can be protected by SECURE_OFF=ON)

Replacement of the HELP.LOG command by the HELP.HISTO command

List of commands, events and system messages at the end of this manual

Harmonisation of the system commands

Introduction to the IP2 system...

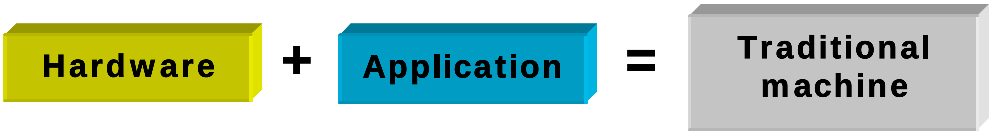
CAUTION: this manual describes the IP2 system and not the equipment in which this IP2 system is included. If you do not know the IP2 system or how IP2 equipment operates, take time to read this document in detail. Otherwise, refer directly to the manual for the actual product, generally called the "user guide".

AZTEC RADIOMEDIA has developed hardware and software architecture that provides what we call ***IP network connectivity*** to its communicating products and to its partners products.

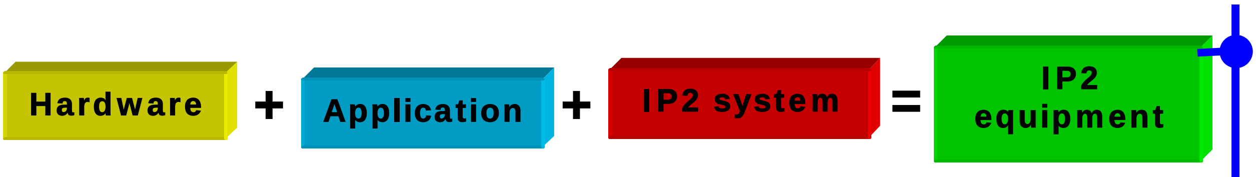
IP networks are innervating companies, organisations and regions. The origin of this success is the opening of the network communication protocol called TCP/IP. Even though it is complex, this protocol has the merit to have been specified publicly and pragmatically. Its components and mechanisms are based on exchanges in "direct" language and not coded.

From now on, network connectivity no longer stops at the computers and printers connected to a company Intranet. Various machines can profit from network infrastructures: in particular, the equipment that has the **IP2 system developed by AZTEC RADIOMEDIA.**

The ***IP2 SYSTEM*** is a communicating software module integrated in electronic ***HARDWARE*** (interface) and associated to an ***APPLICATION*** (software): the combination of these 3 elements leads to ***IP2 EQUIPMENT*** that will be characterised by its ability to communicate over Intranet, Extranet and on the network of networks, i.e. the Internet.



Hardware: this is normally a PCB, associated to various interfaces with the outside world: audio inputs and outputs, relays, logic and analogue inputs, various communications ports... AZTEC RADIOMEDIA is a manufacturer of electronic hardware.



APPLICATION: this is the software that drives the hardware. The application bears the job of the machine, the application knows when to do what and how. AZTEC RADIOMEDIA develops application software or applications for its own products and its clients' products by taking a close interest in the "job of the machine".

In practice, **IP2 equipment**, i.e. hardware that hosts an application and the IP2 system know how to perform the following communicating actions:

- To connect your machine to an Intranet network or the Internet
- To access and configure your machine with a Web Browser
- To consult and recover the history log in the form of a text file
- To work live on your machine on-line via Telnet
- To exchange data organised into files in text format
- To avoid specific cabling by taking advantage of your Intranet
- To plan new perspectives concerning remote control
- To use proven access and exchange security standards
- To make equipment compatible and heterogeneous processes

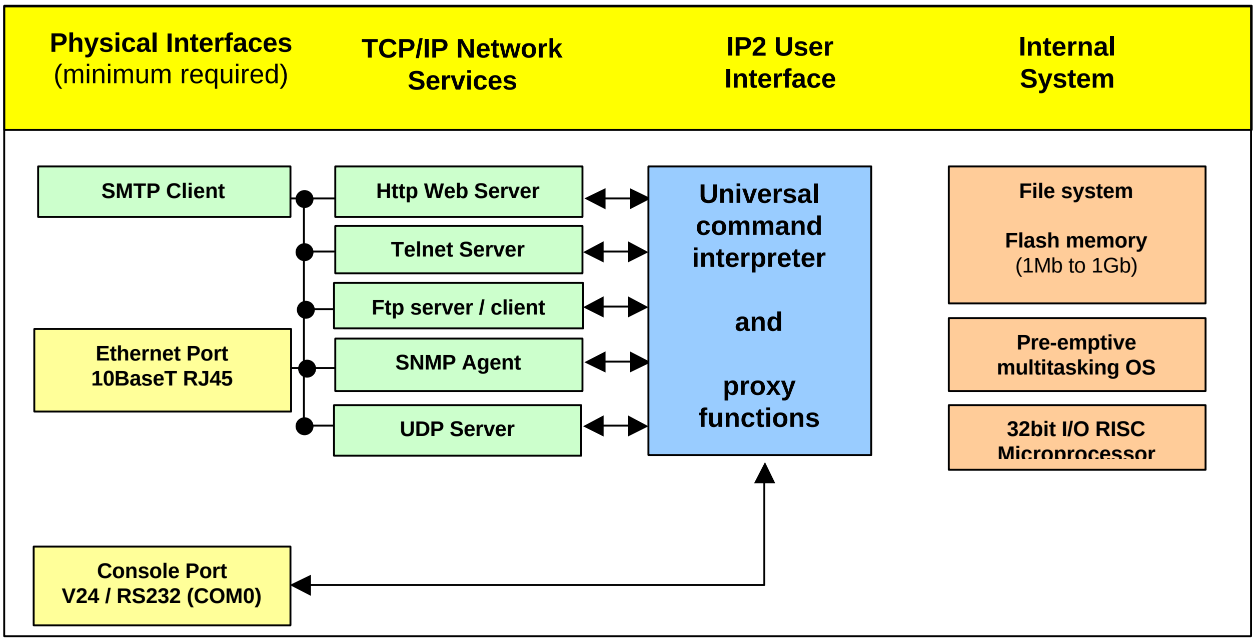
The **IP2 system** is implanted in numerous products developed by AZTEC RADIOMEDIA, a few examples are given below:

- **Alarm systems** made communicative with IP2 and using the network infrastructure to send the events back to a remote station from a few hundred metres to several thousand kilometres away…
- **Intercom systems** use the IP2 system to transmit the speech of 2 correspondents exchanging instructions via an intercom from one point to another. The Intranet network replaces the specific cabling and breaks down the barriers of distance by offering unmatched flexibility to these intercom systems that are very much used in industrial backgrounds.
- **Remote control via network**: turning machines on and off by network, RESETTING equipment
- With IP2, **talking machines** can acquire, record and rebroadcast voice and musical programmes on talking machines. The programs are updated by high-speed file transfer via an Ethernet network.
- **Radio and television transmitters**: distant, inaccessible and sensitive, the transmitter sites today are being equipped with Ethernet network techniques. AZTEC RADIOMEDIA has a complete range of IP2 equipment that allows all the equipment making up a transmitter site to be networked together

- **Lift and boiler room machinery** are so many automated systems with which we would like to be able to interact more rapidly and more reliably. The IP2 equipment developed by AZTEC RADIOMEDIA allows automated systems, regulators and contactors to be driven via computer or technical networks
- **Road traffic regulation systems**: with IP2, the traffic lights in a town can be networked together and can collect a considerable amount of statistical information
- **Weather and air monitoring stations**: the IP2 system is ideally suited to instrumentation and content measurement. Creating history logs and storing measurements in the form of organised files adds to the intelligence of sensors and measurement stations. This equipment is interrogated via the network from any type of machine: MAC, PC, UNIX station.

The IP2 system architecture

"IP2" refers to a range of high-tech products developed by AZTEC RADIOMEDIA that includes very advanced communicating functions in an extremely reduced volume. The figure below shows the architecture of IP2 equipment, concerning both the main hardware and software modules.



The following paragraphs briefly describe the role of each of the modules that makes up the IP2 system.

The IP2 filing system

IP2 equipment always incorporates a memory whose structure is similar to a hard disk or a disk drive. Information is stored in it in the form of files in the same way as that of a computer on its hard disk.

The filing system makes ups the basis of a communicating equipment and gives it power, opening and interoperability with regards to the outside world. In the network field, the capacity of equipment to exchange information remotely and in a standard way is fundamental. Thus, the existence of a filing system enables:

- *HTML pages* to be stored in the form of **HTML files** edited by yourself
- the operation of the Web server (*http*)

- the internal software of the IP2 equipment to be managed as an **executable file**, that can be updated by downloading
- the configuration to be managed in the form of a **configuration file**
- commands written in plaintext in a **command file** to be executed

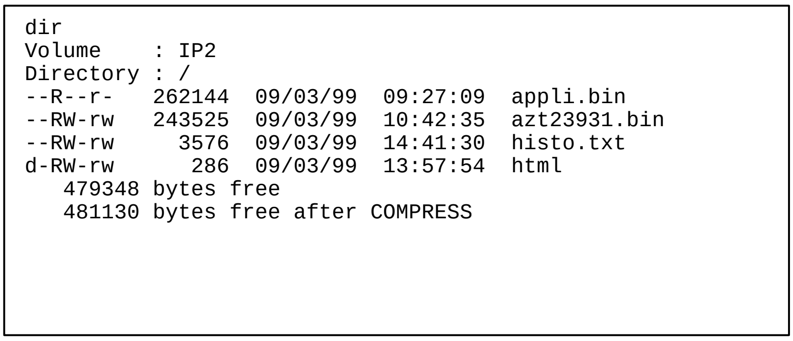
The file system is based on 3 types of memories:

- FLASH memory on the IP2 board
- RAM on the IP2 board (directory /RAM)
- external PCMCIA ATA memory board (ex: FLASH) (directory /ATA)

IP2 equipment has 1Mb to 1Gb of flash memory reserved to actually run the application (configuration files, commands, HTML pages). 700Kb to 1500 KB are reserved for the ***internal software***.

The contents of the flash memory can be viewed in 4 ways:

- via the Console port
- in telnet connection
- in ftp connection
- in http connection



```
dir
Volume    : IP2
Directory : /
--R--r-   262144  09/03/99  09:27:09  appli.bin
--RW-rw   243525  09/03/99  10:42:35  azt23931.bin
--RW-rw     3576  09/03/99  14:41:30  histo.txt
d-RW-rw      286  09/03/99  13:57:54  html
   479348 bytes free
   481130 bytes free after COMPRESS
```

The above figure shows the response to the ***dir*** command sent to the IP2 system by the console port or the Telnet console port: 2 files and 1 directory are present in this example.

Each file is described by a name of 20 characters maximum (including the extension) and by traditional attributes that can be used to reserve or protect their access to a configurable category of users.

IP2 system Web server

The IP2 system incorporates a Web server, i.e. with a simple Browser such as Microsoft Internet Explorer or Netscape' Communicator you can access HTML pages on the network that make up a mini-site web.

The embedded Web server is entirely configurable. Regardless of their origin (Mac, PC, Unix), it can host any type of file such as, for example:

.PDF: Adobe Acrobat documents

.HTM: html documents (pages)

.JPG, .GIF: all image formats

.CLASS: Java applets

.MP3: MPEG2 Layer3 audio files

The publication of files intended for the server is done with the traditional command lines of the FTP protocol or with even more user-friendly tools such as Windows Commander® or Internet Explorer 5. A link to the "Windows Commander" shareware exists on the AZTEC web site at the address http://www.aztec.fr/@ip2fr/ip2_sites.htm

Even better, with your Web browser: you can interact on the system and the application of the IP2 equipment. Indeed, the HTML pages hosted by the IP2 equipment can contain forms or entry fields that can act on the configuration of the system or application. Technically, the IP2 system uses the CGI mechanism.

The IP2 system allows the publication of "**public**" Web pages, i.e. that can be accessed by everyone, without restriction. The IP2 system also allows "**private**" pages to be published i.e. a user name and password are required to enter into the private part of the Web server. The public pages can be used to display parameters, the pages in the private zone of the embedded Web server can allow interactions with the system and the application.

FTP service (File Transfer Protocol)

This service that basically consists of the FTP protocol enables:

- the management of files and directories in the filing system
- the updating of the embedded Web server in the IP2 system
- the updating of the internal program of the IP2 equipment

The IP2 system's embedded FTP server is fully compatible with the various FTP clients on the market. It can be activated in the following ways and/or using the following tools:

Windows 95, 98 and NT native FTP: open a DOS or Command window and type ftp

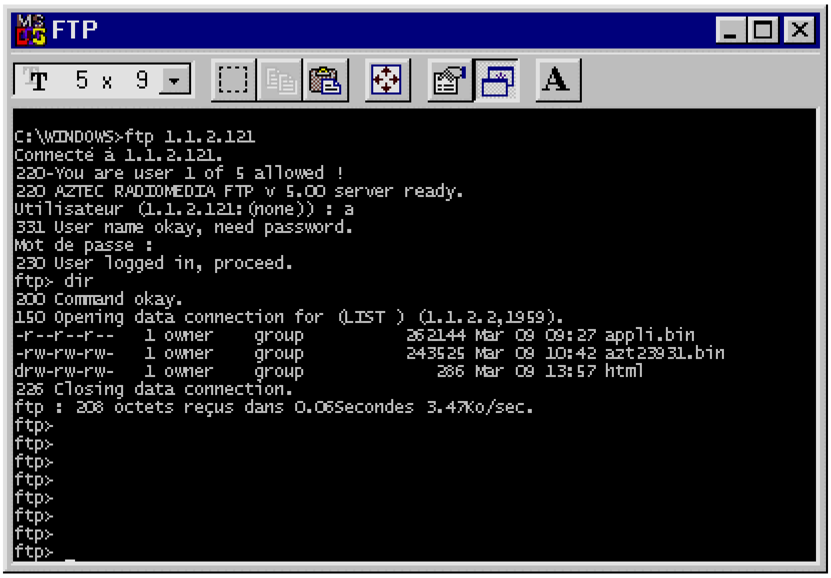
FTP from *Netscape Communicator*: type ftp://[IP address of the IP2 equipment]

FTP from *Microsoft Internet Explorer*: type ftp://[IP address of the IP2 equipment]

FTP from Windows Commander: utility supplied on our CD-ROM, see operating conditions for this software.

The internal software of the IP2 equipment is updated with FTP: this operation can therefore be carried out remotely, without working on site. The updates for the internal software of IP2 equipment can be found on the AZTEC Web site http://www.aztec.fr/support/ip2doc_tec.htm#ip2com_gb.

The access to the IP2 system's FTP server is protected. A ***Login*** (user name) and ***password*** are required to have access to all of the FTP functions. According to the user's authorisation level, he may only be authorised in read-only mode.



```
C:\WINDOWS>ftp 1.1.2.121
Connecté à 1.1.2.121.
220-You are user 1 of 5 allowed !
220 AZTEC RADIOMEDIA FTP v 5.00 server ready.
Utilisateur (1.1.2.121:(none)) : a
331 User name okay, need password.
Mot de passe :
230 User logged in, proceed.
ftp> dir
200 Command okay.
150 Opening data connection for (LIST ) (1.1.2.2,1959).
-r--r--r--   1 owner    group          262144 Mar 09 09:27 appli.bin
-rw-rw-rw-   1 owner    group          243525 Mar 09 10:42 azt23931.bin
drw-rw-rw-   1 owner    group             286 Mar 09 13:57 html
226 Closing data connection.
ftp : 208 octets reçus dans 0.06Secondes 3.47Ko/sec.
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp>
ftp> _
```

The above window is obtained by starting ftp in Windows 98 or NT.

TELNET Service (console mode in IP network)

The TELNET server of the IP2 system allows the following operations:

- access to the set (interpreter) of system and application commands for the IP2 equipment

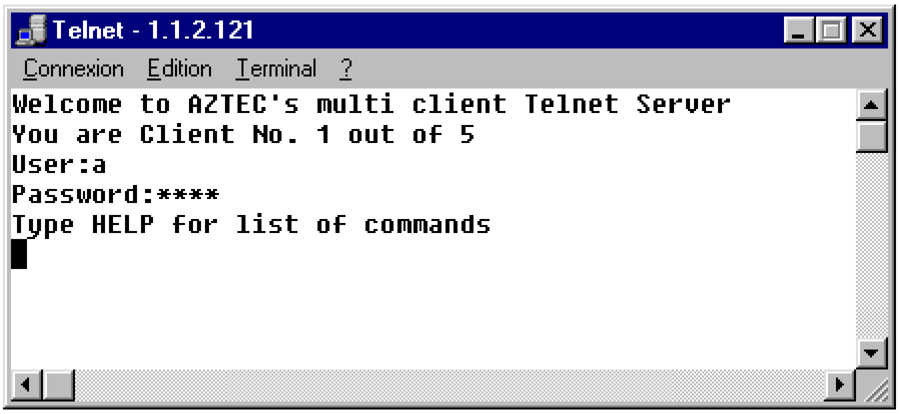
- visualisation of the IP2 equipment's history log file
- configuration of the parameters that determine the equipment's operating mode
- interaction with the specific functionalities of each IP2 equipment

For example, the Telnet server of the IP2 system can be activated with the following tools:

In Win95, 98 or NT: menu start / execute / telnet (on any PC)

In Windows CE: the Rukson "Telnet Force" client (www.rukson.com) operates

From an Internet browser, by typing telnet://



```
Welcome to AZTEC's multi client Telnet Server
You are Client No. 1 out of 5
User:a
Password:****
Type HELP for list of commands
```

The above figure shows an example of what is obtained when you connect to IP2 equipment with the Windows 98 Telnet client. The Telnet server of the IP2 system indicates the number of users ('clients' in network jargon) connected to the appliance at the same time. For all IP2 equipment, the **HELP** command can be used to display the access menu to the various help subjects and the list of commands supported by the command interpreter of the IP2 equipment.

SNMP agent

All IP2 equipment is equipped with an SNMP agent.

Characteristics: MIBII, SNMP V1

A first level of snmp proxy functions is assured via a generic trap **IP2_TRAP** and by the object **IP2_PROXY_COMMAND**. In fact, all the events and all the administration of any IP2 equipment can be done via these 2 objets.

Of course, the IP2 SNMP agent can receive objects, variables and traps specific to a manufacturer MIB. This is the subject of integration work made simple thanks to an MIB compiler: this integration work can be carried out by qualified IP2 integrators or directly by AZTEC.

Contact AZTEC RADIOMEDIA for more information on these IP2 integration subjects: ip2@aztecland.com

SMTP client

The SMTP client assures the possibility of sending an email in response to IP2 events.

UDP services

A multi-port UDP server is implanted in the IP2 system. One of the main advantages of this server is it makes several IP2 appliances addressable at the same time by using the broadcast technique (transmission of audible packets for all the IP addresses in the sub-network). By default, 5 UDP servers are installed in an IP2 appliance, this number can nevertheless vary according to the hosted applications.

By default, the UDP server points to the IP2 command interpreter. Therefore, the data sent to the IP2 equipment via UDP arrives as commands sent to the IP2 command interpreter.

Note: in other IP2 applications, especially in the audio transport field, other UDP servers are created and associated directly to the application without direct link with the UDP servers mentioned in this paragraph.

HELP.UDP displays the commands related to the UDP services

?UDP displays the UDP configurations

UDP<n>.PORT=<n° port> can be used to define the port number associated to the UDP server n°n

UDP<n>.PROTOCOL=ASCII defines a protocol for UDP server n. The IP2 system only provides for the ASCII protocol, connected to the command interpreter. Other protocols can exist according to the application related to the IP2 system.

INIT.UDP reinitialises the UDP parameters to their default values

UDP<n>.USERLEVEL=<ROOT|SUPER|NORMAL> defines the user level associated to server <n>

UDP<n>.FILTER=<x.x.x.x> where <x.x.x.x> is an IP address filter (use '*' to authorise all the values of x). This command can be used to only take into account the requests coming from pre-defined addresses or groups of IP addresses.

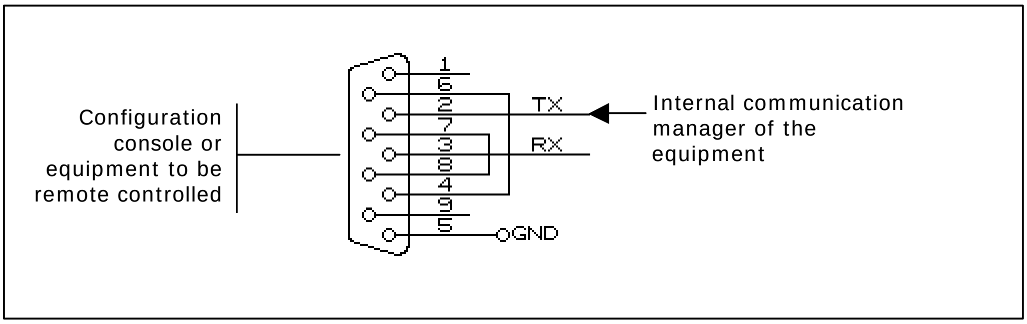
UDP<n>.MODE=<UNI|BIREQ|BI> can be used to define the operating mode of the UDP server.

Physical interfaces (always present)

Console Port

The console port is very often called COM0 on AZTEC RADIOMEDIA products. The user guide specifies which physical port it is. The console port is an RS232 port (V24) DCE (female) accessible on the front or rear panel depending on the product.

A computer can be connected to the IP2 equipment's console port via the ribbon cable normally supplied with the IP2 equipment. In principle, there is no control signal on the console port and the corresponding lines are normally connected in a loop as shown in the figure below:


Configuration console or equipment to be remote controlled
1
6
2
7
3
8
4
9
5
TX
RX
GND
Internal communication manager of the equipment

The Ethernet port

The Ethernet port assures the network hardware connectivity of any IP2 equipment. In principle, an RJ45 connector with isolated signals is implanted on the IP2 products.

In other terms, a twisted pair ribbon cable must connect the IP2 equipment to the router or to the nearest HUB.

The Ethernet port of the IP2 equipment is generally 10BaseT. The information relative to the Ethernet or MAC address associated to the equipment is given in the chapter "to configure the IP address of the IP2 equipment".

Notation conventions

The **commands** that can be addressed to the command interpreter appear in bold, black characters on a yellow background: example **IP=192.167.98.90**

The **events** appear in white characters on a blue background: example **FTP_LOGIN**

The system **messages** appearing in the history log are shown in bold, white on a purple background: example **FTP_ERROR**

🗐 Start-up, system configuration

Before starting up the IP2 equipment, assure that you have understood all the connection details for the equipment in the first chapters of the user guide.

As the IP2 system is common to all the products developed by AZTEC RADIOMEDIA, the principle of network and system configuration is also common to all of this equipment.

It is fundamental to understand the contents of the following paragraphs, regardless of the **IP2** equipment. They must be read carefully, at least once. This information determines the behaviour of the IP2 equipment on the network to which you will connect it.

▲ Before starting!

Each IP2 appliance has a unique serial number in the world that allows it to be clearly distinguished from other Ethernet equipment: this is the MAC address of the product. The MAC address cannot be configured or modified, it represents the "absolute" identifier of the network hardware. Later on, you will see that this MAC address contains the serial n° of the IP2 equipment.

To be able to be located and used on a TCP/IP network, the IP2 equipment must be configured with an ***IP address***. The IP address is to private networks and Internet what the telephone number is for the company telephone networks or the public telephone network. By using the IP address of the IP2 equipment, you will succeed in establishing a connection with the appliance that you wish to remote control.

▲ Caution:

Never connect IP2 equipment to the network without

- informing the Administrator of the network on which you will install the equipment
- configuring the equipment with the IP parameters that were given to you by the network administrator

In every case and especially in the case of a direct connection to Internet, obtain a **fixed IP address** from your access provider or Administrator of your Intranet network so that the IP2 equipment can be permanently accessible on the network.

The default configuration of any IP2 equipment straight from the factory is the following:

Ethernet address (MAC)	**00-90-3F-xx-xx-xx** **where xx-xx-xx is the serial n°** **of the IP2 equipment**
IP address	**IP=192.168.0.1**
Sub-network mask	**MASK=255.255.255.0**
Default router address	**GATEWAY=0.0.0.0**

The IP2 command interpreter

The core of the IP2 system is based on:

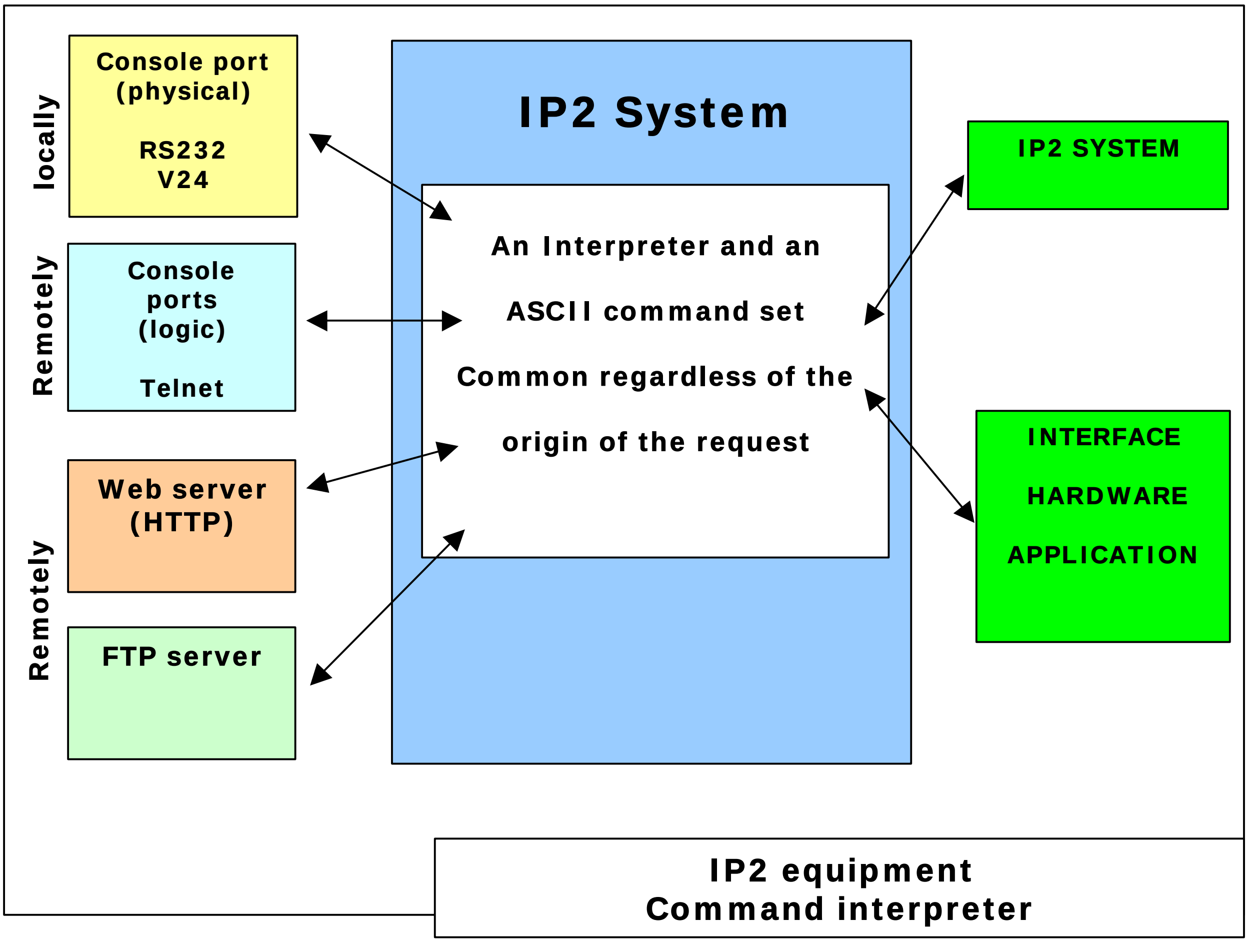
- a multitasking core, (pre-emptive multitasking OS)
- a 32 bit I/O RISC microprocessor
- a multi-client and multi-port command interpreter

The command interpreter interacts with

- the IP2 system
- the application and the interfaces of the equipment

The figure below explains how the command interpreter of the system can be approached by many sources or "ports". For each source, you must have the access rights required to activate the commands.

The commands defined in the IP2 system and the commands related to the application (documented in the user guide) can be used as much in the Web pages (Encrustator® overlay mechanism) as in on-line FTP requests. These subtle mechanisms are clearly described in this manual and assure a unified command set regardless of the port via which this command is initiated. Behind this mechanism, the network specialists can see the pre-requisites to integrate a proxy agent (snmp, http and ftp).



All the commands addressed to the interpreter are done in ASCII code, i.e. in plaintext. The following conventions are respected regardless of the product in the IP2 range and regardless of the AZTEC RADIOMEDIA product.

Notation in the following examples: the indications that appear between brackets **[ ]** are optional. The characters **< >** should never be entered and are simply to help present the syntax of the commands.

The **<CR>** symbol represents the 'code 13' character (chr$(13)) ('\x0D') (Carriage Return)
The **<LF>** symbol represents the 'code 10' character (chr$(10)) ('\x0A') (Line Feed)
The **<TAB>** symbol represents the 'code 9' character (chr$(9)) ('\x09') (Tabulation)

Types and generic syntax of the interpreter commands

To assign a value to a parameter that can be modified by the user:

Console: **<parameter name>=<value><CR>[<LF>]**

Response from the interpreter:

- **+<CR><LF>** if allocation successful
- **!<CR><LF>** if failure or command incorrect

To read the value of a parameter that can be modified by the user:

Console: **<parameter name>?<CR>[<LF>]**

Response from the interpreter:

- <value of the parameter><CR><LF>
- **!<CR><LF>** if command not understood by the interpreter

To read a parameter that CANNOT be modified by the user:

Console: **<parameter name>?<CR>[<LF>]**

Response from the interpreter:

- < value of the parameter ><CR><LF>
- **!<CR><LF>** if command not understood by the interpreter

To perform a particular action:

Console: **<action command>[<list of parameters>]<CR>[<LF>]**

Response from the interpreter:

- **+<CR><LF>** if action performed with success
- **!<CR><LF>** if command not understood by the interpreter

About the Encrustator®: Encrustator® is a technique developed by AZTEC RADIOMEDIA that allows an HTML page (Web page) to be inserted in the source code of the commands to be addressed to the IP2 equipment's command interpreter. Encrustator® goes further and also allows actions to be addressed via CGI commands with the GET and POST methods. These mechanisms are described further in this manual.

To configure the IP address of the IP2 equipment

The configuration of the IP address for the equipment is a prerequisite!

1 configuration via the console port: easy

2 configuration via the network: for the network experts

To configure the IP address via the console port

1. Configure a terminal in 9600,8,N,2 (ASCII) (on the Windows systems, HyperTerminal is suitable)
2. Turn the IP2 equipment off and back on again
3. Using the ribbon cable, connect the console port (physical) of the IP2 equipment to the communication port activated by the terminal or the terminal application
4. Enter the **IP=<x.x.x.x>** command where <x.x.x.x> represents the IP address that your network administrator has attributed to the equipment. Validate with **<Enter>**. The "+" sign tells you that the command sent has been successfully accepted by the system interpreter.

To configure the IP address by ARP request

Caution: this method only works if the IP2 equipment is in the same sub-network as the machine that configures it (station, MAC, PC, ...). It is preferable to send a ping beforehand from the station to a known machine on the same sub-network.

1. Locate the serial n° of the IP2 equipment. It is made up of 3 hexadecimal numbers in the form: **XX-XX-XX** or 6 numbers of the type **00-90-3F-XX-XX-XX**
2. Open a DOS window in Win 95/98/NT and type arp –s <desired IP address> <00-90-3F-XX-XX-XX >

   Example: arp –s 194.132.19.102 00-90-3F-00-00-27
3. Turn the IP2 equipment on and wait about fifteen seconds. If the equipment was already on, turn it off and back on again.
4. Within the minute after turning it on, send a "ping" from the computer to the defined IP address:

   ping <desired IP address>

   Example: ping 194.132.19.102

A message informing you that the PING command was successfully executed will be sent by the system, the response to the first PING to the IP2 equipment always takes a little bit longer (a few seconds) to appear.

On UNIX: use the command
arp - <IP2 equipment name> <Ethernet address> temp

This syntax may vary from one system to another. Consult the manual of your system to be sure of the correct syntax relative to the execution of ARP commands.

To configure the TCP/IP network parameters

Besides the IP address, the IP2 equipment must know other parameters related to the network on which it is connected.

To obtain the list and values of the network parameters for the IP2 equipment, use the **?NETWORK** command

CAUTION: do not forget that the network parameter modifications will only effectively be taken into account after sending the **RESET** command addressed to the IP2 equipment or after an On / Off cycle. This measure allows you to modify the network configuration remotely, without moving. Check the validity of the IP addresses entered before remotely **RESETTING** the IP2 equipment, failing which, you would no longer have access to it on the next attempt to open a session.

The default IP address of the router

Use the **GATEWAY=<x.x.x.x>** command to define the default address of the router. When you use the IP2 equipment on an Internal network without a router, or when you use it on a branch of the network without having to leave this branch, enter **GATEWAY=0.0.0.0** However, if the IP2 equipment must be visible from Internet or another branch of the network to which it is connected, the router supplying that branch of the network must be identified and the IP address of this router must be specified.

The IP address of the IP2 equipment

Once the IP address of the IP2 equipment has been configured the first time, it can be modified again using a command. Use the **IP?** command to read the current value of the IP2 equipment's IP address and the **IP=<x.x.x.x>** command to assign a new value to it.

To define the sub-network mask

The **MASK=<x.x.x.x>** command can be used to define the sub-network IP mask. If no administrator manages your network, we advise configuring this mask in the same way as it is configured on other machines (PC, MAC etc...).

In the other cases, your Internet access provider or your network administrator must specify and know the value of this mask.

Use the **MAC?** command to know the Ethernet address (MAC) of the IP2 equipment

To define the maximum size of the IP packets on the network

The MTU parameter, configurable with the **MTU=<v>** command can be used to force the IP packets not to exceed a given size (expressed in bytes).

Recommended values:

=> **Small LAN without router**: configure MTU to its maximum value <v>=1500

=> **Intranet network** with router: configure MTU to 1500. Reduce this value to 1000 bytes if the network is heavily loaded, or even saturated.

=> the IP2 equipment is connected to the **Internet network** and can be accessed via this network. Configure MTU to a low value, the value 500 is a good compromise and in many cases, will prevent the fragmentation of IP packets on the network and the introduction of delays in routing data.

Name and descriptor of the IP2 equipment

On a TCP/IP network, where everything connected is compatible, nothing looks more like an IP address than another IP address... This means that at first sight, a PC, a router or an IP2 appliance appears equivalent on the network.

Therefore, it is very important to be able to distinguish the IP2 equipment with an explicit label rather than a number. This distinction is made by attributing a name to the IP2 equipment with an additional description, if required.

The name of the IP2 equipment is automatically displayed in the welcome messages of the Telnet and FTP sessions. The name of the IP2 equipment can of course be displayed on the Web pages served by the IP2 equipment. It can also be present in the Email that the IP2 equipment can send so that the recipient will know from "whom" the message came.

In the case where numerous IP2 appliances are operated on a network, we often use the geographical name of the site where each one is installed to make up the name of the equipment.

The name of the IP2 equipment also figures in each history line in the history file '***histo.txt***'.

Use the **MY_NAME=<nom ... >** command to configure the name of the IP2 equipment, 16 characters are authorised, punctuation and accented characters are prohibited. Spaces, figures, lower case letters, upper case letters accepted.

In some cases, we may want to add a comment or a description associated to the IP2 equipment. The text parameter **MY_DESCRI=<cccc...ccc>** is provided for this purpose. Use the parameter as you wish to store a line of 80 characters max, without punctuation or accents.

To protect the access to the IP2 equipment

Level of security

3 levels of access are provided by the IP2 system and are identified by the characters r, s and n, defined as follows:

- **r** (root): has all the rights, including to change and see the *logins* and *passwords*
- **s** (super): has write and read rights to the on-line commands, (telnet, ftp, http)
- **n** (normal): read rights on the main parameters

When the IP2 equipment is delivered, no particular protection is enabled, the equipment is in mode r (root):

- The *login* to be entered is ***root***
- The corresponding *password* is ***root***

Declared users

The management and control of the accesses are configurable in mode ***root*** (r). 10 user profiles with 10 user names (logins) and associated passwords can be saved by the IP2 system.

The command to define and modify these logins and passwords is the following, this command can only be accessed in mode "root" i.e. (r):

USER<n>=<login>,<password>,<level>

When you are at the root level, i.e. when you have all the system rights, it is possible to display the list of users and their profiles with the **?USERS** command
The **USER?** command returns your user level
The **HELP.USERS** command displays the user administration commands.

To protect the access to the console port

A user declared as *root* can disable the access to the physical console port. Use **CONSOLE=OFF**, this command can be accessed via all the input ports of the interpreter.

The physical console port can be re-enabled from all the access ports to the IP2 system interpreter except of course from the actual console port. Use the **CONSOLE=ON** command.

If **CONSOLE=ON** then it is possible to protect the access to the console port by entering the command **LOGOFF_CONSOLE**. Then, on the next connection request, the console port will ask the user to identify himself with his user name and password. Do not use the command **LOGOFF_CONSOLE** if you wish to leave the access to the console port free. The **LOGOFF_CONSOLE** command is available regardless of by which port it is entered (Telnet, FTP, HTTP).

To delete authentication

In some cases, we will want to delete all the authentication requests, either for temporary requirements, or because we consider that there is no risk of hacking on the network:

The commands **SECURE=OFF** and **SECURE_CGI=OFF** can be used to disable (at the *root* level) the authentication requests (login, password) that are displayed during a CGI, Telnet or Console connection. These commands have no effect on the FTP connections, which always require authentication.

To access the help menus

Numerous protocol commands are available in the protocol command set of all IP2 equipment

It is important to differentiate between the commands inherent in the IP2 "system" (those described in this manual) and those inherent in the application that are specified in the User Guide supplied with the IP2 equipment.

By sending the **HELP** command to the system we obtain the list of help subjects:

HELP.SYSTEM: displays the list of commands related to the system
HELP.NETWORK: displays the list of commands related to the IP configuration
HELP.FILE: displays the list of commands related to the filing system
HELP.EVENTS: displays the list of commands related to the event handler
HELP.TIMERS: displays the list of commands related to the timer manager
HELP.WEB: displays the list of commands related to the WEB server
HELP.FTP: displays the list of commands related to the FTP server
HELP.UDP: displays the list of commands related to the UDP clients/servers
HELP.MAIL: list of commands related to the SMTP client (mail)
HELP.SNMP: list of commands related to the SNMP agent
HELP.USERS: list of commands related to the management of the user profiles
HELP.HISTO: list of commands related to the management of the history log file
HELP.APPLI: displays the list of commands specific to the application and the IP2 equipment

To view the parameters by categories

The **?** command can be used to obtain the list of display commands available on each IP2 appliance. Some of these commands have short-cuts, refer to the specific user guide for each appliance.

The following commands are always present regardless of the IP2 equipment:

?NET or **?NETWORK**: displays the IP configuration and the network parameters

?WEB: displays the possible parameters related to the Web server

?ARP: displays the possible parameters related to the ARP table

?TELNET: displays the current Telnet connections

?FTP: displays the possible parameters and status related to the FTP server

?FILE: displays the possible parameters related to the filing system

?UDP: displays the possible parameters related to the UDP clients/servers

?FRAGMENT: displays the data related to the fragmentation of packets (debug)

?MAIL: displays the possible parameters related to the SMTP Mail client

?SNMP: displays the parameters related to the SNMP agent

?USERS: displays the user profiles

?PORTS: displays the active ports

?HISTO: displays the parameters related to the history file

?SYSTEM displays the list of system parameters: time, date, MY_NAME, ECHO, temperature when a temperature sensor is in place etc…

To view the versions of the IP2 services

VER.FTP?

VER.WEB?

VER.AZIO?

VER.AFS?

VER.UDP?

VER.MAIL?

VER.SNMP?

VER.SYSTEM?

VER.BOOT?

VER.CPLD?

AFS.FLASH?

To reinitialise the configuration

Several initialisation commands are provided on each IP2 appliance. The **INIT** command can be used to obtain the list of initialisation commands, the most useful of which are shown below:

INIT.ALL: initialises the equipment to its factory configuration, reserved for the ***root*** user level

INIT.SYSTEM: initialises the system parameters, reserved for the ***root*** user level

INIT.NETWORK: initialises the network parameters

INIT.APPLI: displays the list of initialisation commands available for the application related to the IP2 system.

Actions of the **INIT.NETWORK** command:

```
IP=192.168.0.1
MASK=255.255.255.0
GATEWAY=0.0.0.0
MTU=1500
```

Rights: the initialisation commands can only be accessed at the ***root*** level

The internal clock and how to configure it

The IP2 equipment normally has an incorporated clock and calendar that allows events to be time and date stamped in the history file ***histo.txt***.

The time and date can be configured with the commands DATE=<JJ/MM/AAAA> and TIME=<HH:MM[:SS]>

Use the commands **DATE?**, **TIME?**, **DAY?**, to interrogate the clock.

To enable and disable the echo

By default, the IP2 system command interpreter returns an echo when the command is initiated via traditional consoles to the console port or the Telnet port.

It is recommended leaving the echo enabled (**ECHO=ON**) when you access the system manually. In particular, the echo can be used to check that the IP2 equipment understands the characters that you send it.

If external equipment is driving the console port, it may be interesting to delete the echo so that there is no confusion between the characters returned by the echo and the characters returned by the execution of a command or request.

The echo can be enabled with **ECHO=ON** and disabled by **ECHO=OFF**

Note: the ECHO parameter (console port) is always set to ON, when an IP2 equipment is turned on (except if stated otherwise in the equipment's user manual).

Welcome message on console (COM0) and telnet ports

Welcome message on console port

The transmission of welcome messages (when BOOTING UP and starting the application) on the physical console port (COM0) can be enabled or disabled with the command **WELCOME=ON** or **WELCOME=OFF**.
This measure can be used to avoid disturbing any equipment (modem, console or other) that is permanently connected to this port.

Welcome message on telnet ports

The structure of the welcome message is the following:

Line A: Welcome message containing the equipment name (**MY_NAME?**)

Line B: Information about the client who is connecting (n°)

Line C if **SECURE=ON**: User: <prompt to enter the user name>

Line D if **SECURE=ON**: Password: <prompt to enter the password>

Line E: Prompt to enter **HELP** for on-line help

Line F: **:-)** this sequence chr$(58) chr$(45) chr$(41) chr$(13) chr$(10) marks the fact that the port passes the control to the user who is connected and to the command interpreter. When the access is made by an automatic telnet client (non-manual), this sequence can be used as a marker to start a dialogue with the application.

To remotely "RESET" the equipment

When you are close to the IP2 equipment, the easiest way to RESET the electronics in the equipment is to perform an Off / On cycle.

Remotely, we will use, for example, a Telnet connection to initiate the **RESET** command. The current connection is interrupted after sending the **RESET** command.

Rights: the **RESET** command can only be accessed at the ***root*** level

To obtain information on the version and serial n°

Each IP2 appliance has a unique parameter in the world: this is its Ethernet address, or MAC address. The MAC address of the IP2 equipment is obtained with the **MAC?** command. The serial n° of the equipment is in fact a part of the MAC address and is obtained with the **SN?** command

For all technical support related to equipment incorporating the IP2 system, AZTEC RADIOMEDIA will ask you for the MAC address or the serial number of the product for which you are searching for a solution or information. We will also ask you for the version code of the application software located in the IP2 equipment. This code can be obtained at any moment with the **VER?** command: this command always returns an 8-character code. It exists in the form XXXCCCCV

XXX : sorting key, of no importance (to be ignored)

CCCC : AZTEC reference n°

V : software version, from 0 to 9 then A to Z

AZTEC RADIOMEDIA regularly updates the software of the various IP2 equipment on the market. These updates and the access conditions to these updates are available on the following Internet page of AZTEC RADIOMEDIA's Web site:

ftp://ftp.aztec.fr/support/bin/

🗐 To understand and manage the files

Beyond the parameters – configurable – IP2 equipment is part of the high-tech equipment that incorporates software objects that are more complex than simple parameters, these are **files**.

The file enables various information that is useful to the IP2 system and the application that is based on this system to be accumulated and stored in an organised manner, in plaintext language. The notion of ***file*** offers the possibility of "asynchronous" equipment management: the intelligence of an appliance goes hand in hand with its capacity to order and keep the information within its own system for a period of a few hours to a few months.

In the same way as the appearance of electronic mail has allowed **asynchronous** verbal exchanges that required the presence of 2 interlocutors at the same time, the management of the events and configuration of an IP2 equipment in files avoids it from being in permanent contact at the same time with a server: this results in considerable savings in rented lines, replaced by simple ISDN links (Numéris) for example.

Here are a few examples where the notion of files takes a real dimension.

Talking machines: AZTEC RADIOMEDIA is a specialist in voiced (radio) broadcasting and in particular in talking machines. On the traditional machines of our competitors, voiced messages are broadcast by programming a FLASH EPROM memory using an external programmer. To change the talking messages, the old memory on the board had to replaced by a new one.

The solution proposed by AZTEC RADIOMEDIA exceeds the hopes of our clients: the voiced messages are stored and managed in the form of files, one file corresponding to one voiced message. Updating a message no longer requires changing components but a simple network connection and an FTP transaction (transfer of file(s)).

In many situations, equipment placed on remote sites needed to be permanently supplied with data. We meet this type of situation in the radiobroadcasting field. Traffic data updated every quarter of an hour is in fact permanently transmitted in a loop by a central server destined for remote transmitter centres. The IP2 solution makes the rented lines disappear and entrusts the data encoders (incorporating the IP2 system) with the management of broadcasting from a file.

Result: economically speaking, it is better to transmit N files of 1Ko every ¼ of an hour to different sites and transport the cyclic broadcasting of this file on to each appliance, rather than to manage N very costly permanent communications.

It may seem surprising to see a machine without a hard disk, disk drive, or CD-ROM drive that is capable of structuring its operation around files.

IP2 equipment incorporates a large capacity flash memory, an electronic component, capable of behaving as a real hard disk. The information stored in a flash memory stays in it almost eternally, even after a power-cut. The main advantage of flash memory is it can be erased and reprogrammed which offers an undeniable flexibility relative to fixed systems, based on EPROM components.

Which types of files?

The main files of IP2 equipment:

1. **The 'application' file** called appli.bin . This file contains all the software that makes the IP2 equipment 'work'. When you want to change an IP2 appliance with a new version of software or a specific version, you simply have to download this new version from the AZTEC RADIOMEDIA Web site, then transfer it into the equipment concerned by this update.
   The following chapters explain how to proceed with downloading a new version destined for an IP2 equipment.

2. **The files of web pages**: These files make up and supply the embedded Web server in the IP2 equipment. It can be, for instance, any type of file, text, html, images in Jpeg or GIF formats, sound in MP3 format etc... The following explanations will show you where these files are stored in the filing system and how they can be updated to personalise the embedded web server in the IP2 equipment.

3. **The history file**: this is a file in the text format, with the separator ' ;' that can be read with a text editor or directly with a spreadsheet like Excel.
   The history file is edited each time an event or a system message that is worthy of interest affects the IP2 equipment. A complete chapter is dedicated to the history log, its format and the way in which the corresponding **'histo.txt'** file can be sent back to a server capable of collecting the events accumulated by IP2 equipment or a network of IP2 equipment.

Note that the history file is especially edited during the following events (list non-exhaustive):

- on each power up
- at the start and end of each connection
- on each connection failure
- on each event

To view and work with the files…

The filing system can be accessed in several ways:

- FTP with on-line instructions (FTP commands)
- FTP with Cute FTP or Windows Commander style software
- Telnet with on-line instructions (interpreter commands)
- Console port with on-line instructions (interpreter commands)

It is not the object of this technical manual to describe the FTP instructions and the operation of the software that can be associated to them. The IP2 system responds to the FTP commands in a traditional and standard way.

Besides FTP, some of the IP2 interpreter commands allow the contents of directories and "text" files to be displayed, see below.

The commands available in TELNET are the following:

- **DIR** or **LS** can be used to list the contents of the current directory
- **LS** displays the contents of the directory according to a UNIX style
- **DEL <file>** can be used to delete a specified file
- **COPY <file1> <file2>** copies one file to another
- **MOVE < file1> < file2>** moves a file to another destination
- **CD <directory>** can be used to browse in the tree structure of the directories
- **CD /** can be used to go back up to the top of the filing system's tree structure
- **CD** without argument or the command **CD?** can be used to display the current directory (to know where you are in the filing system)
- **MD <directory>** can be used to create a directory
- **RD <directory>** can be used to delete a directory.
- **MKFS=<volume name>[,<appsize>[,<logsize>]]** the effect of this is to reformat the FLASH EPROM memory and recreate the associated volume. Caution, the effect of this command is to erase all the information present in this memory. Do not use this command

outside possible technical support operations by AZTEC RADIOMEDIA or one of its integrating partners.

Appsize: size of the partition reserved for the internal software /APPLI.BIN (in bytes rounded off to the nearest sector)

Logsize: size of the partition reserved for the history file /HISTO.TXT (in bytes rounded off to the nearest sector)

To defragment the filing system on "on-board" Flash

The IP2 equipment's filing system is based on the use of one or more FLASH EPROM memories located on an IP2 board (does not concern the ATA peripherals or the files in RAM). When a file is deleted or replaced, the space used by the deleted or replaced file is in fact no longer useable straight away, a "hole" is left in the filing system.

The effect of defragmenting the filing system is to delete these "holes" left vacant. **DEFRAG** initiates the defragmentation from Telnet or the console port.

It is possible to ask the IP2 system to automatically defragment the files in FLASH memory when the system starts up with the command **STARTUP_DEFRAG=ON** (OFF to disable this function).

From Telnet, the **DIR** command displays the space free for the files as well as the space free after defragmentation: this information can be used to decide the moment to start the **DEFRAG** command, which in any case, only takes a few seconds.

When you manage your files with FTP (File Transfer Protocol) or with software or an FTP operation browser to handle the files in the IP2 equipment, an error message of the type "disk full" or "disque plein" may appear. In the event of this, do not forget to perform a defragmentation before continuing to handle files.

To observe the current FTP connections

Use the **?FTP** command

FTP connection counter

FTP_CNT? Displays the number of FTP connections accomplished. The command **FTP_CNT=0** sets the counter value to zero.

To update the internal software of the IP2 equipment

Thanks to the comments from our clients and the constant efforts in research and development, AZTEC RADIOMEDIA regularly improves its hardware products by proposing new versions of internal software for the products.

The software version updates for a given product are in principle downloadable from the AZTEC RADIOMEDIA web site at the address **ftp://ftp.aztec.fr/support/bin**

In certain cases, AZTEC RADIOMEDIA creates software versions dedicated to specific applications, particularly for OEM or on-board equipment integrating the IP2 system. Updating these versions, generally specific to an integrator is realised by file attached to electronic mail, no pint in looking for them on our Web site.

The operation to change the internal software is very simple and requires FTP (File Transfer Protocol):

1. Download the latest version of internal software to the IP2 equipment from the AZTEC ftp site, at the address **ftp://ftp.aztec.fr/support/bin**. The corresponding file has a '**.BIN**' extension and is called **<new_version_code>.BIN** where **<new_version_code>** represents the exact reference of this software version.
   Store the **<new_version_code>.BIN** file in a directory identified on your computer.

2. Open an FTP session in line mode
   place yourself directly in the directory where the file <new_version_code>.BIN is located
   In Windows: open a DOS window, type ftp then <Enter>
   Execute the successive commands described below, check that it was executed successfully in FTP

3. Open an FTP session with the IP2 equipment. You must be at the "root" level. Ensure that the access rights are compatible with this operation.
   In Windows: ***ftp < IP address of the equipment>***
   Enter the user name ***<user>***
   Enter the password ***<password>***

4. Once the FTP session is open: Type ***ls*** or view the files in the main directory of the IP2 equipment. You should see 2 files appear with the **.BIN** extension.

   One of the files with the '.**BIN**' extension is called **APPLI.BIN**: this is the internal program that is currently running. The other file with the .BIN extension should be deleted, this is a backup copy of APPLI.BIN

   Use the FTP command ***del /<file to be deleted>*** *to delete the backup copy*

5. Defragment the filing system of the IP2 equipment

   quote (enter mode ftp source)

   site defrag (defragmenting command sent to the command interpreter)

6. Enable the FTP chatterbox mode de to view the progression of the download

   hash (enables the FTP 'chatterbox' mode)

7. Download the .BIN update file to the IP2 equipment

   put <new version file>.BIN /<new version file>.BIN

8. Transfer the application

   quote

   site APPLI=/<new version file>.BIN

9. Quit FTP

   bye

It is possible, for example, to automate these commands in an FTP-SHELL file (Windows) called for example, *upl_ip2.txt*: Open a DOS window or create a shortcut by starting ***ftp -s:upl_ip2.txt***

🗐 To customise the embedded web server

Before attacking this chapter dedicated to customising the embedded Web server in the IP2 equipment, ensure that you have read the presentation of the Web server in the first part of this document.

Note that the Web server of the IP2 system can be disabled and enabled with:

WEB_SERVER=OFF and WEB_SERVER=ON

Web homepage

The homepage is called ***index.html*** in the filing system and is always located in the directory /html

This page is sent by default by the Web server of the equipment when it is accessed with a Web Browser.

This page can be customised according to the rules fixed in this chapter.

"Error" page sent in case of error or page not found

When a requested Web page provokes an error (non-existent page for example), the file **@error.htm** in the directory /html is always returned, if this file and/or this directory do not exist, it/they is/are created automatically. It contains information relative to the error encountered by the server. This file can be customised according to the same rules as those stated in this chapter.

Public pages and restricted access pages

The Web pages likely to be served by the IP2 server can either be public, or restricted access.

The pages placed in the **/html directory** of the IP2 equipment are said to be public as they are served by the IP2 system in all cases without requesting identification.

The pages placed in the **main directory** are also served by the IP2 system but after authentication of the user (user name + password) if the access protection has been enabled by **SECURE=<ON|OFF>**.

Priorities: when a file with the same name is located in each of these directories, the public page is served.

Range of the authentication: As long as a Browser has not been closed, it normally remembers the password entered by the user, thus the authentication request is performed once for all the files.

CGI requests and authentication: it should be noted that as soon as a CGI request is sent to the server, an authentication is also requested from the client who is connecting (if the parameter **SECURE_CGI=<ON|OFF>** is enabled)

To update the Web server

The files of the embedded Web server are updated in an FTP session with the rights to write in the filing system.

We recommend defragmenting (**DEFRAG** command) the equipment's filing system before and after updating the Web server files of the IP2 equipment.

Implied link addresses and explicit link addresses

When the embedded Web site in the IP2 equipment consists of several pages linked together with hypertext links, you should only use relative and not absolute links.

It is recommended using absolute links as opposed relative links to establish links between files in the public directory (/html) and those of the restricted access directory (and vice versa).

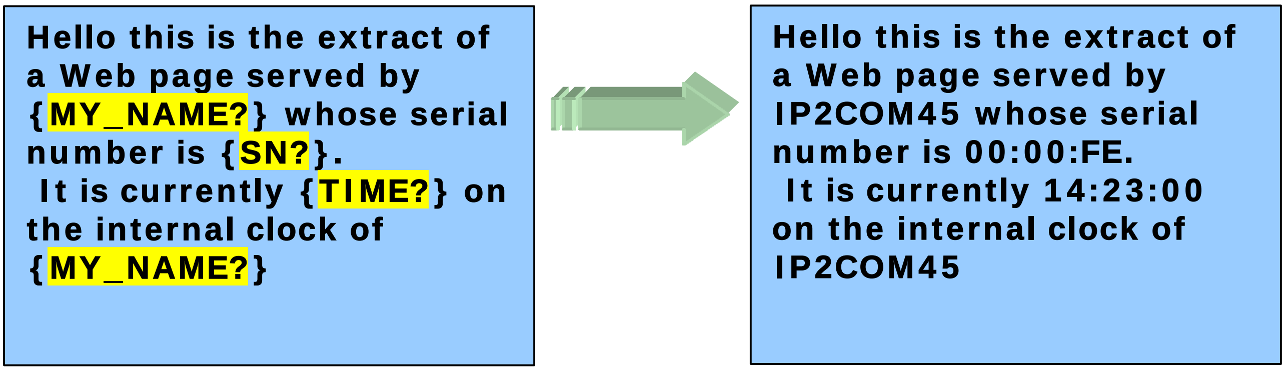
For any hypertext link, image or element pointing outside the IP2 equipment Web site, no restriction of syntax should be considered in as much as these links do not interrogate the Web server of the IP2 equipment.

To display parameters in a page of the embedded server

AZTEC RADIOMEDIA has developed an overlay process called Encrustator®. This process can be used to place instructions in the Web pages of the embedded site that call the command interpreter of the IP2 system: these instructions are executed and the result is overlaid instead of the syntax of the request.

The figure below shows the overlay mechanism. To the left, the original text as it appears in the HTML page saved in the IP2 Web server, to the right, this text as it appears once it is served by the equipment's server. The character strings that are shown between the brackets **{ }** indicate that the contents must be addressed to the command interpreter of the IP2 equipment. The server automatically substitutes these brackets and their contents with the result of the command.

For experienced users, note that the overlay technique can apply to any type of HTML text in the middle of filenames, flags or CGI requests.



Hello this is the extract of a Web page served by {MY_NAME?} whose serial number is {SN?}.
It is currently {TIME?} on the internal clock of {MY_NAME?}

Hello this is the extract of a Web page served by IP2COM45 whose serial number is 00:00:FE.
It is currently 14:23:00 on the internal clock of IP2COM45

IMPORTANT: Underlying aspects to this overlay technique exist and in particular the management of the files by the browser (client) in its cache memory. To tell the embedded server to serve an HTML page in every case and prevent the browser from using its cache memory to display the page, **the filename associated to this page must begin with the character @**. In this way, we can be sure that the HTML page will be loaded from the IP2 server and the overlaid commands and not from the local cache memory which would result in the overlays not being refreshed. This comment also concerns the pages that contain CGI forms (cf. following paragraph).

To execute commands from an HTML form

The IP2 web server incorporates CGI management of forms. The CGI orientated forms make a request on the embedded Web server likely to make an action on the equipment. Due to this, any new CGI request made from one of the Web pages served by the embedded Web server implies an authentication request (Once per http browser session).

You can configure the web server to request user authentication, prior to executing the command. The command **SECURE_CGI=ON** or **SECURE_CGI=OFF** can be used to achieve this configuration.

The Web server of the IP2 system that allows commands to be transferred to the interpreter of the IP2 system, via the forms, is always done according to the following code:

```
<form action="<Page to be returned after executing the CGI>" name="name indifferent"
method="POST">
.. ..
.. code specifying the different fields of the form
..
</form>
```

Note that the action (field *action=*) of the form must always contain the filename relative to the page that the server must return once the CGI commands have been executed. We can also specify the page name ***@interpreter.htm*** to return details relative to the CGI process performed.

The name of the form defined by the field ***name=***, is of no importance.

The commands to be addressed to the interpreter via a form are encoded inside the form according to the following rules applicable to each type of form element. The following examples can be used to highlight the behaviour of each form element when this form is posted by pressing its submit button.

Hidden assignment in a form

When the button below is pressed, the command **MY_NAME=Hello** is sent to the command interpreter of the IP2 system. Note the use of a hidden field to host the command. The ' :' that appears in the ***name*** field tells the IP2 system that the following string 'MY_NAME' is the name of a parameter to be assigned with the argument found in the ***value*** field: when posting a form, the contents of the ***name*** field and the contents of the ***value*** field are associated to make up the string ':MY_NAME=Hello'. On receiving the form, the web server of the IP2 system will detect the character ' :' at the string header and will conclude that the command **MY_NAME=Hello** must be routed to the interpreter. When no argument has passed in the ***value*** field, only the contents of the ***name*** field are addressed to the command interpreter

```
<form method="POST" action="@exemple.htm">
  <input type="hidden" name=":MY_NAME" value="Hello">
  <p>
  <input type="submit" value="MY_NAME=Hello !!!" name="B1">
</p>
</form>
```

Hidden command in a form

When the button below is pressed, the **RESET** command is sent to the command interpreter of the IP2 system. Note that the value field is empty and in this case the RESET name is considered as a command, no argument is then associated to the contents of the ***name*** field.

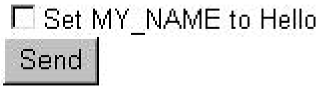
```
<form method="POST" action="@exemple.htm">
  <input type="hidden" name=":RESET" value="">
  <p>
  <input type="submit" value="Press here for RESET" name="B1">
  </p>
</form>
```

To use the check boxes

The check box is often used to enable or disable a process through a variable. Its use for the management of commands is nevertheless not recommended as only the "box checked" information is sent back to the embedded web server when the form is posted.

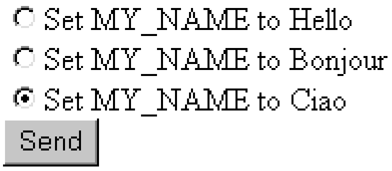
This is inherent in the web browser. Therefore, we will prefer a pair of option buttons rather than a check box to assign a 2-state variable.

In the following example, the command **MY_NAME=Hello** is only sent back to the web server if the check box is selected.



```
<form method="POST" action="@exemple.htm">
  <p>
    <input type="checkbox" name=":MY_NAME" value="Hello">Set MY_NAME to Hello<br>
    <input type="submit" value="Send" name="B1">
  </p>
</form>
```

To use the ‘option’ buttons



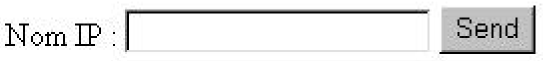
○ Set MY_NAME to Hello
○ Set MY_NAME to Bonjour
● Set MY_NAME to Ciao

```
<form method="POST" action="@exemple.htm">
  <p>
   <input type="radio" value="Hello" name=":MY_NAME">Set MY_NAME to Hello<br>
   <input type="radio" value="Bonjour" name=":MY_NAME">Set MY_NAME to Bonjour<br>
   <input type="radio" value="Ciao" name=":MY_NAME" checked>Set MY_NAME to Ciao<br>
   <input type="submit" value="Send" name="B1">
  </p>
</form>
```

In this example, only the command **MY_NAME=Ciao** is sent back to the web server when posting the form.

To use a text area

In this example, the value entered in the text area is associated to the name of this area (here MY_NAME) to form the command that will reach the command interpreter once the form has been posted.



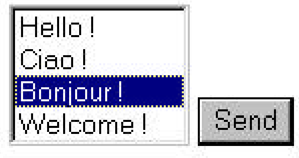
Nom IP :

```
<form method="POST" action="@exemple.htm">
  <p>
    Nom IP : <input type="text" name=":MY_NAME" size="16">
    <input type="submit" value="Send" name="B1">
  </p>
</form>
```

To use a pull-down menu

In this example, each option field constitutes, by the value field, one of the alternatives out of the N options offered to make up the corresponding command. The name of the ***select*** field (here:MY_NAME) is associated to the selected option (here Bonjour ! which refers to the value option *bonjour*).

The command that will be sent back to the command interpreter will therefore be: MY_NAME=bonjour in the example below, once the form has been posted.



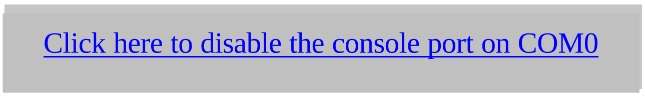
```
<form method="POST" action="@exemple.htm">
 <p>
    <select name=":MY_NAME" size="4">
       <option value="hello">Hello !</option>
       <option value="ciao">Ciao !</option>
       <option value="bonjour">Bonjour !</option>
       <option value="welcome">Welcome !</option>
    </select>
   <input type="submit" value="Send" name="B1">
 </p>
</form>
```

To execute commands from an HTML link

It is possible to address commands to the command interpreter of the IP2 system by simply clicking on hypertext links.

The principle follows rules that are similar to those described in the chapter dealing with sending commands within forms.

The following link disables the console mode on the console port of the IP2 equipment if you click on it:



Click here to disable the console port on COM0

The HTML code of this link is:

```
<a href="page.htm?:CONSOLE=OFF">
        Click here to disable the console port
</a>
```

page.htm is the name of the file to return at the end of executing the command by the interpreter of the IP2 equipment.

To associate several commands in a form

The IP2 Web server accepts of course more than one command per form.

Note that the first command executed is the one whose definition is the first one encountered in the HTML page.

Transactional forms

In the previous examples, the means of addressing the system and the IP2 equipment by means of commands built from form elements was described.

By mixing the possibility of addressing commands to the system and recovering an existing configuration with the overlay system, we easily make user-friendly forms that assure the link between the user of the product and the IP2 system + its associated equipment.

The code of the form below allows a few system parameters to be viewed and configured. Note that the name of its HTML page must begin with @ to authorise the overlay mechanism.

```
<form method="POST" action="@exemple.htm">
  <p>Serial number of the equipment: {SN?}<br>
  <input type="text" name=":MY_NAME" size="16" value="{MY_NAME?}"> : IP2 name<br>
  <br>
  <input type="text" name=":IP" size="20" value="{IP?}"> : IP address<br>
  <input type="text" name=":MASK" size="20" value="{MASK?}"> : Mask<br>
  <input type="text" name=":GATEWAY" size="20" value="{GATEWAY?}"> : Gateway<br>
  <input type="text" name=":MTU" size="20" value="{MTU?}"> : MTU parameter<br>
  <br>
  Configuration of the console :
  <input type="radio" value="ON" name=":CONSOLE" {:CONSOLE?:ON:checked}>Enabled, &nbsp;
  <input type="radio" value="OFF" name=":CONSOLE" {:CONSOLE?:OFF:checked}>Disabled<br>
  <br>
  <input type="checkbox" name=":WEB_CNT" value="0">Set the Web counter to 0<br>
  <br>
  <input type="submit" value="Mettre à jour" name="B1"></p>
</form>
```

Note the use of the overlay principle to display the current configuration inside the actual input areas.

In this form, to set the corresponding option button to its value, we use a special overlay command to make the ***checked*** directive statement appear, whose syntax is the following:

{:<commande>:<string tested>:<string if test ok>[:<string if test not ok>]**}**

- The command ***<commande>*** is addressed to the IP2 interpreter
- If the response to this command is the same as <string tested>
  => then all of the syntax {...} is replaced by <string if test ok>
  => otherwise all of the syntax {...} is replaced by <string if test not ok>

The same principle is used to define which of the fields in a pull-down menu must be pre-selected.

Beware of the cache memories in browsers!

Caution, not all browsers react in the same way to the requests generated by the user. The "cache memories", both at the link level and at the page level, can stop all the elements of a page from being refreshed.

The effect of using Shift+Reload on the Netscape and Internet Explorer browsers is to completely reload the current page and its elements, without recapturing the files and data contained in the cache memory.

Web counter

A counter accessible by the command **WEB_CNT?** can be used to display the number of HTTP requests before resulting in the transmission of a page in HTML format (extension HTM).

The command **WEB_CNT=0** (from the root access level) can be used to reset the counter to zero.

Message and file sending system

Until now, we have described the IP2 system as a server (Telnet, FTP then HTTP). Now, lets examine the way in which the IP2 equipment can behave as a "CLIENT" in relation to a server connected on the network.

IP2 equipment, seen as clients can perform the following operations:

- send a file to an FTP server (FTP client function)
- send an EMAIL to a recipient via an SMTP server (SMTP client function)
- send an SNMP trap to an SNMP manager (SNMP agent function)

To spontaneously send an Email

To send an Email, the IP2 system needs information on the following parameters:

- Enable email sending by: **SMTP.ENABLED=ON**
- The IP address <sss.sss.sss.sss> of the SMTP mail sending server
  SMTP.IP=<sss.sss.sss.sss>

- the number of attempts before declaring a failure to contact the server
  SMTP.RETRY=<number of attempts>

- the duration between 2 attempts to contact the SMTP server
  SMTP.RETRY_TIMEOUT=<duration>

- The return address in case of email return due to a recipient problem. Note that this address – contained in the email message– is taken on charge by the SMTP server and not by the IP2 equipment.
  SMTP.RETURN=<email address>

In some cases, the SMTP server requires prior authentication from the message sender via SMTP. This process requires successfully setting up a connection to the POP3 server associated to the SMTP server. If ***POP3.USER*** is different from an empty string, then a prior connection to the POP server is made before any connection to the SMTP server.

- The IP address of the possible POP3 server

  POP3.IP=<sss.sss.sss.sss>

  <user consists of 8 characters max, beware of the distinction between upper case and lower case characters >

- the name of the POP3 user account

  POP3.USER=<user>

  <user consists of 8 characters max, beware of the distinction between upper case and lower case characters >

- the POP3 password

  POP3.PWD=<password>

  <password consists of 8 characters max, beware of the distinction between upper case and lower case characters >

These parameters can be initialised to their default values with the command **INIT.MAIL**
The IP2 version of the MAIL client can be obtained by **VER.MAIL?**
Important: it is always the last time that the email was sent that is taken into account, no queue is managed. The SMTP server must be present for any request from the SMTP client that is the IP2 equipment.

The IP2 equipment identifies itself with its name **MY_NAME?** in all the emails it sends. The subject of the message is labelled in the following form:

Message from {MY_NAME?} - {DATE?} {TIME?} (© IP2)

The IP2 system knows how to write the email with a text file **<file>** (*.txt), html (*.htm) intended for one or more recipients. This file can appear in the attached form i.e. directly in the body of the email (use the options -A or -T, -T by default).

The command to be addressed to the interpreter in order to send the contents of the file **<file>** as an Email to the list of recipient(s) is the following:

SEND_EMAIL=<email address #1>,...[,<email address #m>][:<file>][-A][-T] (#m possible up to #8)

Note 1: if the name of the text file starts with @, the operation **SEND_EMAIL=...** enables the detection of commands overlaid in the file <@file> (Encrustator system to the same operating rules as those described in the sending of the HTML pages).

It is then recommended placing the following commands in this file that keep the memory of the last event generated: **{EVENT?}**, **{EVENT_REF?}**, **{EVENT_VAL?}**, **{EVENT_DESCRI?}**.

Sending an email can be associated to the occurrence of an IP2 event. Refer to the 'event handling' chapter for more information.

To spontaneously send a file

Caution*: function in project stage, not implanted for the moment, planned in version 1.5 of the system*

To send a file to a recipient, the IP2 equipment behaves in FTP client (File Transfer Protocol) towards a server (the recipient).

- the number of attempts before declaring a failure to make contact with the server
  FTP_CLIENT.RETRY=<number of attempts>

- the duration between 2 attempts to contact the FTP server
  FTP_CLIENT.RETRY_TIMEOUT=<duration>

The following command is to be used to send a file **<file>** to a remote server whose IP address is **<sss.sss.sss.sss>** under the name **<dest file>**:

SEND_FILE=<sss.sss.sss.sss>,<user>,<password>,<file>,<dest file>,[append]

User, Password: user name and password

Note 1: if the **append** option is added, the contents of <file> (file stored in IP2) is added to the end of the file <dest file> on the FTP server.

Note 2: if the name of the text file starts with @, the operation **SEND_FILE=...** enables the detection of commands overlaid in the file @<file> (Encrustator system to the same operating rules as those described in sending HTML pages).

It is then recommended to overlay the following commands that keep the memory of the last event generated: **{EVENT?}**, **{EVENT_REF?}**, **{EVENT_VAL?}**, **{EVENT_DESCRI?}**.

The transmission of files can be associated to the occurrence of a certain IP2 event. Refer to the ‘event handling’ chapter.

To spontaneously send SNMP Traps

The IP2 equipment contains an SNMP agent. An "**IP2_TRAP**" trap has been defined. This IP2 generic trap can be transmitted on the occurrence of an event initiated by the IP2 system or commanded by the external equipment (transmission of traps in proxy mode).

The TRAP IP2_TRAP is specified in ASN1 notation, in association with the variables describing the event as follows, for more details, consult the AZTEC IP2 manufacturer MIB: IP2_MIB.MIB available on request:

```
aztec OBJECT IDENTIFIER ::={enterprises 4651}
IP2_TRAP TRAP-TYPE
      ENTERPRISE  aztec
      VARIABLES   {
                   event_code,
                   event_ref,
                   event_val,
                   evant_descri,
                   event_time,
                   event_date
                  }
      DESCRIPTION
      " This trap is a generic trap generated to send back any IP2 event. The
      transmission of this trap can be requested by the external equipment with
      the command EVENT.MAKE… »

      ::= 0
```

The transmission of IP2_TRAPs can be configured for each type of IP2 event.

The IP address of the SNMP manager can be configured for each type of IP2 event.

The **SNMP.TRAPS=<ON | OFF>** command can be used to enable or disable the transmission of traps from the SNMP agent in a global way. (Do not forget to start the SNMP agent with **SNMP.AGENT=ON**)

Example:

We wish to send a test trap of IP2_TRAP type destined for an SNMP manager located at the IP address 192.178.3.34

- We authorise the **TEST_TRAP** code IP2 event to generate a TRAP destined for the 192.178.3.34 manager. To do this, we send the command **EVENT(TEST_TRAP).SNMP=192.178.3.34**
  The file /IP2EVENTS/TEST_TRAP.EVE is then created by the system and has a line of the type SNMP=192.178.3.34
- We ensure that the system is authorised to generate SNMP traps with **SNMP.TRAPS=ON**
- We create the IP2 event with the command **EVENT.MAKE=TEST_TRAP;;;This is a test**
  When the event appears, the SNMP IP2_TRAP (MIB AZTEC) TRAP will be generated for the SNMP manager at the defined IP address.

To send SNMP Traps commanded externally (proxy trap)

The generation of a generic IP2 TRAP (IP2_TRAP) can be commanded from the console port, some logic inputs of IP2 equipment or via Telnet entries. The generation of these traps is associated to the generation of a user event with the **EVENT.MAKE…**. command. See the events handling chapter for more details.

SNMP administration

To configure the IP2 SNMP agent

- Enable / disable the agent: **SNMP.AGENT=ON|OFF**
- Define the communities authorised to read: **SNMP.COMMUNITY.GET=<text>**
- Define of the communities authorised to write: **SNMP.COMMUNITY.SET=<text>**
- Enable the transmission of traps: **SNMP.TRAPS=ON|OFF**
- Configure the manager IP address by default: **SNMP.IP=<x.x.x.x>**

MIB reference standard

The MIB standard MIB-II specified by rfc1213 is implanted in the IP2 system.

The IP2 AZTEC manufacturer MIB (company number 4651), ASN1 file: IP2_MIB.MIB available on request.

The SNMP ip2_proxy_command Object

The **ip2_proxy_command** object defined in the AZTEC MIB, allows an SNMP manager to access to all the commands in the IP2 system's command interpreter.

For the communities authorised to read, the manager's rights are those of the user declared as ***Normal*** for the IP2 system. (cf. USERS)

For the communities authorised to write, the rights of the manager are those of the user declared as ***Super*** for the IP2 system. (cf. USERS)

The following extract of the AZTEC MIB illustrates the proxy mechanism relative to the IP2 interpreter. Caution, this extract is given as an illustration, you must refer to the AZTEC IP2 MIB to create your applications.

```
aztec OBJECT IDENTIFIER ::={enterprises 4651}
ip2_system OBJECT IDENTIFIER ::={aztec 1}
ip2_proxy_command OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..32000))
   ACCESS read-write
   STATUS mandatory
   DESCRIPTION
   "
   the effect of SET on this object is to address a command to the IP2 system
   command interpreter.
   the effect of GET on this object is to recover the response returned in the
   character string.
   All the transactions are done through strings, the manager is responsible
   for carrying out the conversion operations.
   "
   ::={ip2_system 1}
```

NOTE: note that this does not constitute the ideal method to manage equipment by SNMP. The **ip2_proxy_command** object was implanted to allow access to all the IP2 system variables and the application commands of the various AZTEC and integrator products.

IMPORTANT: The **ip2_proxy_command** object is applicable to all the IP2 system variables and also to all the interpreter commands linked to applications developed with the system by AZTEC RADIOMEDIA and its integrating partners.

For example, the **ip2_proxy_command** object allows an IP2COM (one of the network gateway products developed by AZTEC) to make requests on the V24 – RS232 communication ports of the gateway: this is achieved with the commands of the IP2 "NETCOM" application **COMx.SEND…**

Advanced "SNMP proxy agent" functions

AZTEC RADIOMEDIA develops and integrates proxy agents in all the OEM IP2 cards and some IP2 products providing the link between the network and external equipment.

The theoretical description of interfaced equipment by IP2 can be associated to the IP2 system. AZTEC RADIOMEDIA has an company MIB compiler, capable of generating the code required to load the theoretical model of remotely controlled equipment into the OEM IP2 cards.

Contact AZTEC RADIOMEDIA for more information concerning MIB hosting and its snmp proxy functions in the OEM IP2 cards.

IP2 message and event handling

What is an IP2 event

The IP2 equipment is extremely communicative. It is important to have traces of the connections that it has initialised or accepted. It is also very interesting to record any event of the application likely to provide its user with information.

Connecting a user in a Telnet session, disconnecting him, turning the IP2 equipment back on, updating the internal software are as many examples of system **events** that punctuate the operation of IP2 equipment.

IP2 events specific to a type of IP2 product or associated to an OEM IP2 board can be defined and generated.

An event does not necessarily mean "incident", nevertheless, a communication incident or a network incident are part of the possible events manageable by all IP2 equipment.

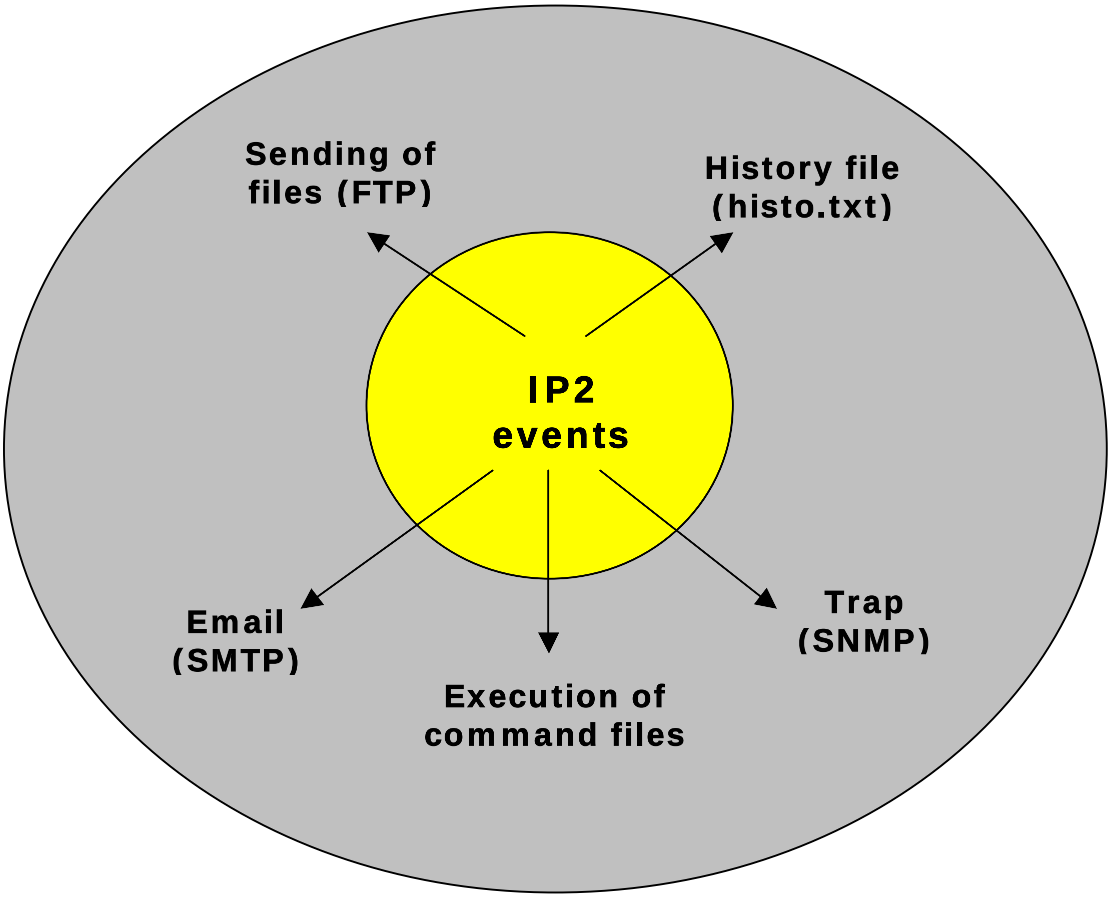
The event library is specified in the IP2 system (this manual), the events related to the applications using the IP2 system are specified for each equipment model. An event is identified by a string of 16 characters max: numbers and characters, without any upper case / lower case distinction, no punctuation characters or spaces.

The notion of event is closely related to the notion of alert and history. That's why IP2 places the event in the centre of the standard alert system:

- Transmission of "IP2_TRAP" SNMP trap
- Transmission of e-mail
- Transmission of a file which can contain contextual elements on the event
- Memorisation of the event in the history file histo.txt
- Execution of a command file specific to each event

What is a IP2 system message

Besides the IP2 events, information messages known as "system messages" can be generated by the IP2 system. They can not be related to a particular action and are written in the history file for information if **LOG_MESSAGES=ON**.
See the end of the manual for the list of system messages.



Error messages and history

Some events are generated by the IP2 system without actually being able to generate the transmission of an e-mail, file, trap or the execution of a command file. These events are normally generated in case of error (impossible to reach the SNMP manager for example). These types of messages are stored in text format in the history file /histo.txt, located in the main directory of the IP2 system.

To generate a user event

Any IP2 event code can be generated with the command EVENT.MAKE=. In the following paragraph, you will see that it is possible to make up a "user" event library, each one with its own properties.

An event that has the <CODE_EVENEMENT> code is generated with the following command and syntax:

EVENT.MAKE=<CODE_EVENEMENT >;<Value>;<Reference>;<Description>

<value>: The value field (ASCII text) contains a possible value related to the origin of the event (ex: temperature value)
<Reference>: the reference value (ASCII text) contains a possible threshold value that was crossed and thus caused the event in question
<Description>: the description field is a free text field, 255 characters max. If the event is written in the history file, only the 80 first characters of this field will be taken into account.

To configure the properties of the events

When an event called <CODE_EVENEMENT> appears, the IP2 system scans the /IP2EVENTS directory to look for the file <CODE_EVENEMENT>.EVE : this file contains, several lines in ASCII form whose object is to define the scripts to be executed when the event <CODE_EVENEMENT> appears.

SNMP=<IP address of the SNMP manager that receives the IP2_TRAP trap>
This line can be used to specify the address of the SNMP manager to which the IP2_TRAP (cf. AZTEC MIB) trap is sent. If no address is specified, no trap is sent.

FTP=<sss.sss.sss.sss>,<user>,<password>,<file>,<dest file>,[append]
This line can be used to specify the destination of the file to be sent if an event is received. To do this, an FTP server is contacted by the IP2 system at the IP address <s.s.s.s>. The IP2 system identifies itself with <user> and <password> then sends the file <file> from its local filing system to the destination file <dest file>.

SMTP=<address email#1>…[,address email#m][:<file>][-T] [-A]
This line follows the same syntax as the one specified for the second body of the instruction SEND_EMAIL, that is:
<email address#1>…[,<email address#m>][:<file>][-A][-T] (#m possible up to #8)

The transmitted e-mail is in the format specified in the chapter dedicated to sending e-mails.

HISTO=ON | OFF
Determines if the event must or must not be written in the IP2 system history file /histo.txt.

BATCH_FILE=<command file to be executed having the extension>[.CMD]
Specifies the name of a command file .CMD to be executed for on the occurrence of a given event.

The <CODE_EVENEMENT>.EVE file is created automatically, if it does not already exist. It is created from the model file /IP2EVENTS/TEMPLATE.EVE

You can configure TEMPLATE.EVE with a default configuration. If the TEMPLATE.EVE file does not exist, it is automatically created with the following content:

```
SNMP=
FTP=
SMTP=
HISTO=ON
BATCH_FILE=
```

These files can be configured by downloading or by using the following ASCII commands that will modify the contents of the corresponding line in the file:
/IP2EVENTS/<CODE_EVENEMENT>.EVE

```
EVENT(<CODE_EVENEMENT>).SNMP=...
EVENT(<CODE_EVENEMENT>).FTP=...
EVENT(<CODE_EVENEMENT>).SMTP=...
EVENT(<CODE_EVENEMENT>).HISTO=...
EVENT(<CODE_EVENEMENT>).BATCH_FILE=...
```

The commands to reread these configurations are:

```
EVENT(<CODE_EVENEMENT>).SNMP?
EVENT(<CODE_EVENEMENT>).FTP?
EVENT(<CODE_EVENEMENT>).SMTP?
EVENT(<CODE_EVENEMENT>).HISTO?
EVENT(<CODE_EVENEMENT>).BATCH_FILE?
```

Where is the history file, how is it displayed?

The history file is a file in text format that can be read directly via Telnet or the console port, or, once repatriated, with a text editor or better still, with a spreadsheet.

The file is called **HISTO.TXT** and is located in the main directory of the filing system.

The **HISTO.TXT** file can be displayed in several different ways:

- Via Telnet or the console port, using the command **TYPE HISTO.TXT**
- With a Web browser: http://<sss.sss.sss.sss>/histo.txt where sss.sss.sss.sss represents the IP address of the IP2 equipment. (authentication requested)
- By recovering the file **HISTO.TXT** during an FTP session.

Size and uniqueness of the history file

The history file of the IP2 system is unique. This uniqueness takes into account that spreadsheets are tools of unrivalled power for statistical processing, sorting, organising and presenting results: the IP2 equipment stores a complete history file and the centralising system is charged with organising these results.

The size of the history file in an IP2 appliance is fixed at 64Ko as standard when creating the volume in the FLASH memory. This value can be changed by recreating a volume in the FLASH memory (see filing system chapter in this manual).

The format of the history file allows:

- HISTO.TXT to be read and used with a spreadsheet
- history files from different sources to be linked together, particularly files from all AZTEC RADIOMEDIA IP2 equipment

The history file can be deleted in Telnet or via the console port (**DEL HISTO.TXT**) or during an FTP session.

What happens when the history file is full?

No management of the history file is required. In practice the size of the file is configured when the flash memory is formatted with the MKFS command.
When the history reaches its maximum size, it is divided into two parts, and the older part is deleted.
It is possible to set a maximum size threshold for the history file with the command **HISTO_LIMIT=<ratio>**. This ration is given in respect to the maximum size of the history file /HISTO.TXT. When this threshold is passed, the system generates the **HISTO_LIMIT** event. You then can configure the IP2 system to send back an alert or even the actual history file to a manager or server.

To specify the format of the history file HISTO.TXT

Each line of the history file HISTO.TXT refers to an event. Each line of the history file is divided into fields separated by semicolons (**;**). The field marked "1" is the first field in the line, the list of the fields is defined as follows:

Field 1	**{DATE?}**	**Event date**	**YYYY/MM/DD**
Field 2	**{TIME?}**	**Event time**	**HH :MM :SS**
Field 3	**{MY_NAME?}**	**Equipment name**	**16 characters max**
Field 4	**{SN?}**	**Batch N°**	**XX-XX-XX**
Field 5	**Event code** **{EVENT?}**	**Event code**	**16 characters max**
Field 6	**Reference value** **{EVENT_REF?}**	Fields reserved for the application. Consult the **user guide** of the equipment concerned.	**16 characters max**
Field 7	**Event value** **{EVENT_VAL?}**		**16 characters max**
Field 8	**Comment** **{EVENT_DESCRI?}**		**80 characters max**

Event code: This is the name of the event and the command file (.CMD) associated to this event. See the list of event codes managed by the IP2 equipment in the paragraph of this chapter dedicated to this subject.
Reference value, event value: in some cases, the generation of an event results in monitoring a parameter relative to a given reference.

Comment: The event is often accompanied by peripheral information that is often related to the origin of the event. This information often appears in this text area, which does not exceed 80 characters.

The "RESET" events

The **RESET** event has an important place in the log (history file) of any IP2 equipment. It helps you understand the causes that have generally contributed to generating an equipment **RESET**.

The possible reasons for the RESET are shown in the comment area of the history file:

- RESET voluntarily generated by the system: SW RESET
- RESET generated by the hardware watchdog: HW RESET
- RESET generated by the software watchdog: SW WDOG
- RESET generated on power up: POWER UP, POWER OFF YY/MM/DD
  - RESET generated by the clock disappearing : LOSS CLK

Note that it is possible to know the length of a power supply interruption by analysing the **RESET** event for a voltage drop cause: the time and date of the voltage drop appear in the comment area associated to the event.

The TIMER, NEW_DAY, NEW_HOUR events

The system is equipped with 3 TIMERs: TIMER1, TIMER2 and TIMER3. These clocks can be used to generate events at regular and programmable intervals.

The 3 timers can be managed and configured by the following commands:

TIMER<n>=ON

TIMER<n>=OFF

TIMER<n>.PERIOD=< cycle length of the timer concerned in minutes>

TIMER<n>.RESET

TIMER<n>? displays the value (minutes) of timer n

<n> represents the Timer n° concerned between 1 and 3

Each time a TIMER cycle finishes, the **TIMER1**, **TIMER2** or **TIMER3** event is generated, it is then possible to configure the properties of these events to make them send an e-mail, trap etc... (command: EVENT(TIMER1).SNMP... for example), see the chapter dedicated to event handling in this manual.

It should be noted that some applications use specific timers and that they can also generate events.

The **NEW_DAY** and **NEW_HOUR** events are generated on the transition from one day to the next or one hour to the next respectively, observed on the IP2 equipment clock. The **NEW_DAY=[ON | OFF]** and **NEW_HOUR=[ON | OFF]** commands can be used to enable and disable the generation of these events.

Example: To program an IP2 appliance to send an E-mail everyday using TIMER2

The following example explains how to send the history file of the IP2 equipment everyday (1440 minutes) to the Email address toto@wanadoo.fr

- Configure TIMER2:

  TIMER2=ON

  TIMER2.PERIOD=1440

- On station or PC, create the command file TIMER2.CMD with a conventional text editor and enter, for example, the command:

  SEND_EMAIL=<toto@wanadoo.fr>:/histo.txt-T

The "LOG" events

The **LOG** events can be used to trace the connection activity on the various standard accesses of the IP2 system:

- Connection to the embedded FTP server
- Connection to the embedded Telnet server
- CGI connection on the embedded Web server

Each authenticated connection and disconnection (login + password requested on connecting) generates a LOG_ON or LOG_OFF event.

The declared events are the following:

FTP_LOGIN: start of FTP connection

FTP_LOGOUT: end of FTP connection

FTP_LOGFAIL: end of FTP connection

TELNET_LOGIN: start of Telnet connection

TELNET_LOGOUT: end of Telnet connection

TELNET_LOGFAIL: failure of Telnet connection

CONSOLE_LOGIN: start of console session

CONSOLE_LOGOUT: end of console session

CONSOLE _LOGFAIL: failure of Console connection

Additional indications relative to the connection (user, IP address, etc…) may appear in the comment field of the event lines in the history file

"SYSTEM" messages

The **LOG_MESSAGES=<ON | OFF>** command can be used to stop the IP2 equipment from writing the system messages in the history file.

The events will always be written on the condition that the .HISTO property of the event is set to ON.

Command files

The command files are executed in 2 possible ways:

1. Explicit method with the command **COMMAND <command file>[.CMD]**
2. Implied method by the occurrence of an event containing the property .BATCH_FILE filled in with the command file in question

- The command files called on the occurrence of events (method 2) must be located in the directory /IP2EVENTS
- The command files must have the extension .CMD and must only contain valid commands in ASCII format, one command per line
- Empty lines in the command file are ignored
- A line beginning with ***//*** is considered as a comment and is ignored
- The command **COMMAND <command file name >[.CMD]** can be used to manually execute a command file.
- It is possible to define a wait state of a few seconds between 2 commands with the system command **WAIT=<number of ms>**
- On certain IP2 boards, it is possible to emit successive and rapid beeps with the function **BEEP=<t>[,n]** where ***t*** represents the duration of the beep in ms and ***n*** the operating mode where 0=continuous and 1=pulse.
- It is recommended ensuring that only one command file can be executed at a time, the system nevertheless allows several executions at the same time. The command COMMAND can be located inside a command file, but preferably at the end.
- The embedded command files lead to parallel and not sequential executions.
- The execution result (trace) for the last 100 commands coming from executed command files is located in the directory+file /RAM/BATCH_HISTO.TXT. This result is made up of lines, each one corresponding to an executed command, 3 fields:
  - o Command file from where the command comes
  - o Date and time that the execution of the command started
  - o Reminder of the command sent to the interpreter

- The interpreter's response to the command. Only the first 20 characters of the response are saved

Memo of commands, events & messages

IP2 system commands

Help commands

HELP

HELP.EVENTS

HELP.TIMERS

HELP.MAIL

HELP.SYSTEM

HELP.NETWORK

HELP.FILE

HELP.WEB

HELP.FTP

HELP.UDP

HELP.SNMP

HELP.USERS

HELP.HISTO

HELP.APPLI

Viewing commands

? displays the list of viewing commands

?NET or **?NETWORK**: displays the IP configuration and network parameters

?ARP: displays the possible parameters related to the ARP table

?TELNET: displays the current Telnet connections

?FTP: displays the possible parameters related to the FTP server

?FILE: displays the possible parameters related to the filing system

?WEB: displays the possible parameters related to the HTTP web server

?TIMERS: displays the possible parameters related to the timers

?MAIL: displays the possible parameters related to the SMTP Mail client

?SNMP: displays the parameters related to the SNMP agent

?UDP: displays the parameters related to the UDP server

?USERS: displays the user profiles

?PORTS: displays the active ports

?HISTO: displays the history file

?SYSTEM displays the list of system parameters

To know the software versions of the services

VER?

VER.FTP?

VER.WEB?

VER.AZIO?

VER.AFS?

VER.UDP?

VER.BOOT?

VER.CPLD?

AFS.FLASH?

VER.MAIL?

VER.UDP?

VER.SNMP?

VER.SYSTEM?

Initialisation commands (accessible in ROOT mode only)

APPLI=<internal binary program file>.BIN update the application

APPLI.FORCE=<internal binary program file>.BIN forced update of the application without verification

BOOT=<boot binary program file>.BIN forced update of the boot

BOOT.FORCE=<boot binary program file>.BIN forced update of the boot without verification

MKFS=<volume name>[,<appsize>[,<logsize>]] flash memory formatting

MY_NAME=<IP equipment name> identification of the IP2 product or the IP2 board

MY_DESCRI=<additional description> description of the IP2 product

INIT displays the initialisation commands

INIT.ALL general initialisation

INIT.TIMERS disables the events related to the 3 TIMERS

INIT.UDP initialises the UDP servers

INIT.APPLI displays the list of initialisation commands for the application

INIT.USERS initialises the user parameters to their default value

INIT.SNMP initialises the SNMP agent parameters to their default value

INIT.WEB initialises the WEB server parameters to their default value

INIT.MAIL initialises the EMAIL parameters to their default value

INIT.SYSTEM initialises the system parameters, reserved for the ***root*** user level

INIT.NETWORK initialises the network parameters

RESET micro reset

RESTART_APPLI restarts the APPLI.BIN application

Date and time

DATE=<JJ/MM/AAAA> defines the date

TIME=<HH:MM[:SS]> defines the time

DATE? displays the date

TIME? displays the time

DAY? displays the day (3 letters)

Network configuration

IP=<x.x.x.x> defines the IP address

MASK=<x.x.x.x> defines the sub-network mask

GATEWAY=<x.x.x.x> defines the gateway

MAC? displays the MAC address

SN? Displays the serial number of the hardware deduced from the MAC address

MTU=<v> configures the MTU

WEB server configuration

WEB_SERVER=ON|OFF enables or disables the WEB server

WEB_CNT? Reads the Web counter

WEB_CNT=0 sets the Web counter to zero

FTP server configuration

FTP_CNT? reads the Web counter

FTP_CNT=0 sets the Web counter to zero

Telnet server configuration

WELCOME=ON|OFF enables or disables the welcome message in telnet

SNMP agent configuration

SNMP.AGENT=ON|OFF Enables / disables the SNMP agent

SNMP.COMMUNITY.GET=<text> defines the communities authorised in reading

SNMP.COMMUNITY.SET=<text> defines the communities authorised in writing

SNMP.TRAPS=ON|OFF enables or disables the SNMP traps

SNMP.IP=<x.x.x.x> IP address of the SNMP manager by default

Commands related to event handling

EVENT? displays the code of the last event

EVENT_REF? displays the reference value associated to the last event

EVENT_VAL? displays the value associated to the last event

EVENT_DESCRI? displays the description accompanying the last event

EVENT(<CODE_EVENEMENT>).SNMP=<SNMP manager IP address>

configures the SNMP trap to be transmitted on the appearance of the <CODE_EVENEMENT> event

EVENT(<CODE_EVENEMENT>).FTP=<s.s.s.s>,<user>,<password>,<file>,<dest file>,[append]

configures sending a file on the appearance of the <CODE_EVENEMENT> event

EVENT(<CODE_EVENEMENT>).SMTP=<email address#1>...[,email address#m]:<file>[-T] [-A]

configures sending an EMAIL on the appearance of the <CODE_EVENEMENT> event

EVENT(<CODE_EVENEMENT>).HISTO=ON | OFF

configures writing the <CODE_EVENEMENT> event in the history file /HISTO.TXT

EVENT(<CODE_EVENEMENT>).BATCH_FILE=<command file>[.CMD]

configures executing a command file on the appearance of the <CODE_EVENEMENT> event

EVENT.MAKE=<CODE_EVENEMENT >;<Value>;<Reference>;<Description>

Generates the <CODE_EVENEMENT> event with its associated arguments

Commands related to timer event handling

TIMER<n>=ON | OFF starts | stops the TIMERn, n=1 to 3

TIMER<n>.PERIOD=<period of the timer concerned in minutes> period of the TIMERn

TIMER<n>.RESET=<reinitialise the period of the timer concerned> resets TIMERn to zero

TIMER<n>? query current value of the TIMERn (minutes)

NEW_DAY=[ON | OFF] enables the NEW_DAY event on the change of day

NEW_HOUR=[ON | OFF] enables the NEW_HOUR event on the change of hour

Commands related to the management of command files

COMMAND <file>[.CMD] executes a command file

WAIT=<number of seconds> wait state in a command file

BEEP=<t>[,n] emits a beep if buzzer present on IP2 board

Commands related to the filing system

DEL <file> deletes a file

COPY <file1> <file2> copies a file

MOVE <file1> <file2> moves a file

CD <directory> changes directory

CD.. moves up to the parent directory

CD/ to enter the root directory of the filing system

MD <directory> creates a directory

DIR lists the current directory

DIR <path> lists a designated directory

TYPE <text file> displays the contents of a text file

ATTRIB <file | directory> [H],[R],[W],[h],[r],[w] modifies the attributes of a file | directory

DEFRAG defragments the files in the FLASH memory

STARTUP_DEFRAG=ON|OFF defragments the files automatically at start-up

HISTO_LIMIT=<ratio> maximum size of the /HISTO.TXT file before event

Commands related to the management of users and access rights

USER<n>=<login>,<passwrod>,<level> creates a user profile

USER? What rights (user level) do I have ?

?USERS displays the user profiles

SECURE=ON|OFF enables or disables the authentication request in Telnet and private Web files

SECURE_CGI=ON | OFF enables or disables the authentication request during CGI execution

Commands related to the management of the physical console port

CONSOLE=ON | OFF enables or disables the physical console port

LOGOFF_CONSOLE quits an open session on the physical console port

Commands related to the management of E-mails (SMTP)

SMTP.ENABLED=ON enables the transmission of E-mails

SMTP.IP=<sss.sss.sss.sss> IP address of the SMTP server

SMTP.RETRY=<number of attempts> number of attempts before abandoning sending email

SMTP.RETRY_TIMEOUT=<durée> time between 2 attempts to send an EMAIL

SMTP.RETURN=<email address > email return address if recipient cannot be found

POP3.IP=<sss.sss.sss.sss> IP address of the POP3 server, useful if authentication required

POP3.USER=<user> user name if POP3 authentication required, otherwise empty

POP3.PWD=<password> password if POP3 authentication required, otherwise empty

SEND_EMAIL=<email address1>[,<email address2>][, etc...]>[:<file>][-A][-T]

Send an EMAIL with a file attached or in the body of the EMAIL

Commands related to the management of UDP servers

HELP.UDP to view the commands related to the UDP services

?UDP to display the USP configurations

UDP<n>.PORT=<port n°> can be used to define the port number associated to the UDP server n°n

INIT.UDP reinitialises the UDP parameters to their default values

UDP<n>.USERLEVEL=<ROOT|SUPER|NORMAL> user level associated to the server <n>

UDP<n>.FILTER=<x.x.x.x> filter for authorised addresses

UDP<n>.MODE=<UNI|BIREQ|BI> operating mode of the UDP server.

UDP<n>.PROTOCOL=ASCII protocol supported by the UDP server n (ASCII by default).

IP2 system events

FTP_LOGIN: start of FTP connection

FTP_LOGOUT: end of FTP connection

FTP_LOGFAIL: end of FTP connection

TELNET_LOGIN: start of Telnet connection

TELNET_LOGOUT: end of Telnet connection

TELNET_LOGFAIL: Telnet connection failure

CONSOLE_LOGIN: start of console session

CONSOLE_LOGOUT: end of console session

CONSOLE _LOGFAIL: Console connection failure

RESET: system reset, cf. associated message to understand the context

TIMER1: the TIMER1 has terminated and is starting to count again

TIMER2: the TIMER2 has terminated and is starting to count again

TIMER3: the TIMER3 has terminated and is starting to count again

NEW_DAY: change of day

NEW_HOUR: change of hour

HISTO_LIMIT: alert when the size of the history file has exceeded the HISTO_LIMIT threshold

IP2 system messages

The messages are written in the history file only. They are not considered as events and cannot generate an email, trap or the execution of command files.
This list of system messages is non-exhaustive. The following list constitutes the most interesting messages.

AFS_CREATE: formatting the flash memory

UPDATE: updating the internal software, successful

UPDATE_ERR: updating the internal software, unsuccessful

UPDATE_BOOT: updating the BOOT software, successful

UPDATE_BOOT_ERR: updating the BOOT software, unsuccessful

TELNET_ERROR : error in the ip2 TELNET server application, cf. attached message

TELNET_WARNING : warning in the ip2 TELNET server application, cf. attached message

FTP_ERROR : error in the ip2 FTP server application, cf. attached message

FTP_WARNING : warning in the ip2 FTP server application, cf. attached message

FTP_OPEN : IP2 application open: FTP server

FTP_CLOSE : IP2 application closed: FTP server

HTTP_ERROR : error in the http (web) ip2 server application, cf. attached message

HTTP_OPEN : IP2 application open: HTTP server

HTTP_CLOSE : IP2 application closed: HTTP server

MAIL_SEND : started to send email

MAIL_ERROR : error on sending an email, cf. associated message

MAIL_END : email successfully sent

DEL_HISTO : the history file has been manually deleted by a user (cf. message)

HISTO_FULL : message coming from the system indicating that a part of the history file has been deleted (the oldest part) in order to free the flash memory.

TASK_ERR : error in the creation of services (cf. message)

IP2 hardware architectures

The **OEM IP2** boards have been developed to enable product and system designers to quickly integrate TCP/IP Ethernet network connectivity. With the IP2 system, the IP2OEM boards provide your solution with all of the low level network functions as well as the high level TCP/IP services.

The NETCOM functions integrated as standard in the OEM IP2 boards, enable your appliance to be immediately shown on the IP network. If the interfaced equipment communicates in ASCII via a V24-RS232 port, it becomes immediately accessible via TELNET, SNMP and via the HTML Encrustator© function developed by AZTEC RADIOMEDIA. Your equipment will then serve HTML pages and knows how to respond to the requests from an SNMP manager.

The OEM boards are opportunities for OEM development partnerships. For a programmer in C language, it takes less than a day to get to grips with the IP2 development environment. In a few hours programming, you can give your product the ability to send personalised EMAILS and SNMP TRAPS. The IP2 system also gives your solutions a complete event handler that allows a history file to be edited and consulted.

The IP2OEM board can also be used as a development platform for more advanced OEM integration: the IP2OEM board is used as a daughter-board and carries drivers dedicated to the equipment that it remotely controls. Developing snmp proxy agents becomes a real pleasure and company MIB accumulation is then possible. The completely configurable extension port allows the IP2OEM board to assure all the micro functions of the appliance that hosts it.

The IP2 system, hardware and software architecture integrates almost 20 years of development experience. A lot more than a simple TCP/IP stack, it integrates the OS, the filing system and a hardware solution ready to be used by your networked equipment.

IP2OEM board (PC104 format)

Main characteristics

- Board in PC104 format (electrical and mechanical)
- Low cost and easy to implement
- Ethernet 10BaseT
- Native IP2 system
- Possibilities of extension to the outside world:
  - 16 bit PC104 BUS
  - or 8 bit PC104 BUS + 28 generic I/Os
  - or 80 generic I/Os
- Single-voltage power supply: 5V
- Mounting on daughter-board
- 2 communication ports
- Integrated NETCOM function: gateways RS232, V24 Network
- Buzzer

Applications

- Provides network connectivity to existing equipment
- Input output management systems
- Radio – TV transmission equipment
- Audio equipment
- Alarm and security systems
- Remote sites

Operational characteristics

- Complete standard IP2 system
  - TCP/IP
  - Servers: http (web), ftp, telnet
  - Clients: smtp (mail), sntp (time), ftp
  - Agent: SNMP, MIB-II + MIB AZTEC
  - Filing system in RAM and FLASH memories
  - Event handler and history manager
  - Secure access, 3 levels
  - Updating of BOOT application by FTP
  - Updating of application by FTP
- Pre-emptive multitasking OS
- Complete IP2COM application integrated for the generic OEM boards
  - Proxy agent http, incrustation
  - Virtual V24 extension via TCP/IP network
- Specific application developed for OEM contracts
- Applications can be hosted on the IP2OEM board for OEM contracts
  - Proxy-agents SNMP, TELNET, HTTP
  - Various I/O interfaces
  - Driving of complex boards
  - Various MMI
  - Audio

Physical characteristics

- Dimensions:
- Position of the mounting holes:
- Weight:

Power supply

- Single-voltage: 5,00V +/- 5%
- Consumption: 400mA typ.
- Connectors: via extension connector or bi-point

Memories and peripherals

- Static RAM: 1Mo
- FLASH: 4Mo
- E2PROM: 32Ko
- Backed up RAM: 8Ko
- Calendar clock

Microprocessor

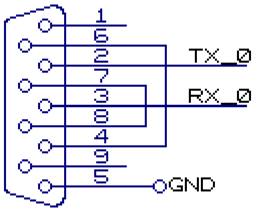
- Motorola: 68EN360
- Clock: 25MHz

Ethernet

- RJ45 connector
- 10BaseT
- Isolation by transformer
- Pre-configured MAC address

Port COM0: RS232 V24

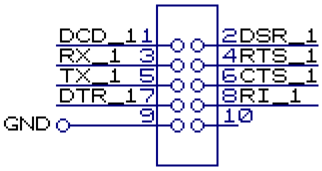
- HE10 connector
- Direct compatibility with SUBDB9 connector
- Provided for output on female SUBD connector, one-to-one cable
- Protection against common mode voltages: yes
- Signals: RX and TX only on this port



RS232 - COM0

Port COM1: RS232 V24

- HE10 connector
- Direct compatibility with SUBDB9 connector
- Provided for output on male SUBD connector, one-to-one cable
- Protection against common mode voltages: yes
- Signals: RX, TX, DCD, DTR, DSR, RTS, CTS, RI



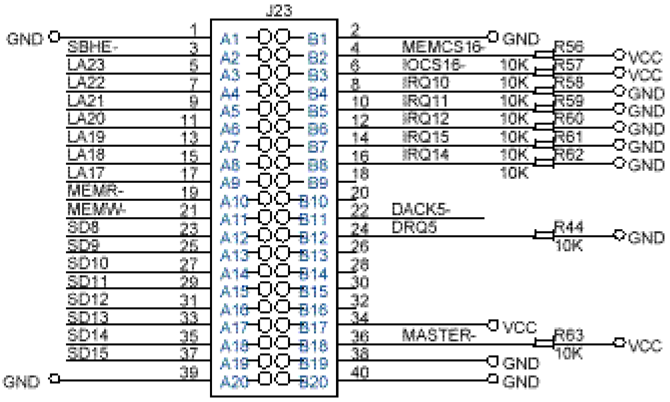
RS232 - COM1

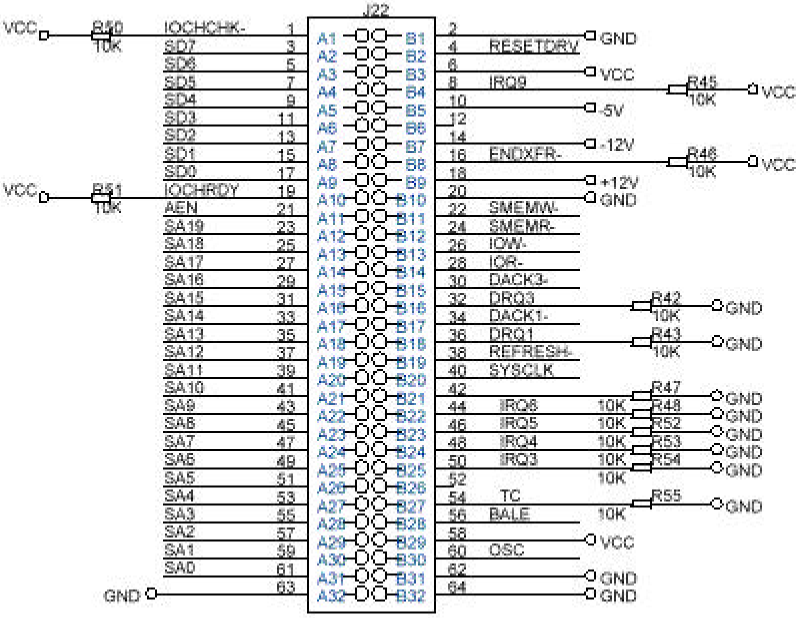
Miscellaneous

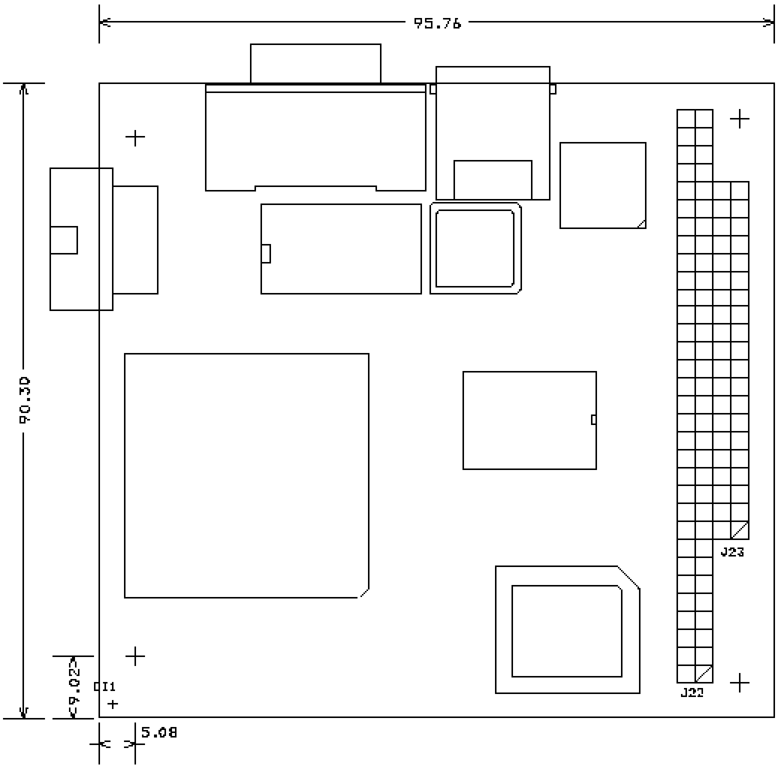
- Buzzer integrated on the board
- JTAG port for internal CPLD schematic reloading for extension connector
- 2 input ports for button or external dry contact (TTL pull-up)
- LEDs
    - o 4 signalling LEDs (2 red, 2 green)
    - o 3 network LEDs: tx, rx, col

PC104 connector

- Connector


J23
GND 1 A1 B1 2 GND
SBHE- 3 A2 B2 4 MEMCS16- R56 VCC
LA23 5 A3 B3 6 IOCS16- 10K R57 VCC
LA22 7 A4 B4 8 IRQ10 10K R58 GND
LA21 9 A5 B5 10 IRQ11 10K R59 GND
LA20 11 A6 B6 12 IRQ12 10K R60 GND
LA19 13 A7 B7 14 IRQ15 10K R61 GND
LA18 15 A8 B8 16 IRQ14 10K R62 GND
LA17 17 A9 B9 18 10K
MEMR- 19 A10 B10 20
MEMW- 21 A11 B11 22 DACK5-
SD8 23 A12 B12 24 DRQ5 R44 10K GND
SD9 25 A13 B13 26
SD10 27 A14 B14 28
SD11 29 A15 B15 30
SD12 31 A16 B16 32
SD13 33 A17 B17 34 VCC
SD14 35 A18 B18 36 MASTER- R63 10K VCC
SD15 37 A19 B19 38 GND
GND 39 A20 B20 40 GND


J22
VCC R50 10K IOCHCHK- 1 A1 B1 2 GND
SD7 3 A2 B2 4 RESETDRV
SD6 5 A3 B3 6 VCC
SD5 7 A4 B4 8 IRQ9 R45 10K VCC
SD4 9 A5 B5 10 -5V
SD3 11 A6 B6 12
SD2 13 A7 B7 14 -12V
SD1 15 A8 B8 16 ENDXFR- R46 10K VCC
SD0 17 A9 B9 18 +12V
VCC R51 10K IOCHRDY 19 A10 B10 20 GND
AEN 21 A11 B11 22 SMEMW-
SA19 23 A12 B12 24 SMEMR-
SA18 25 A13 B13 26 IOW-
SA17 27 A14 B14 28 IOR-
SA16 29 A15 B15 30 DACK3-
SA15 31 A16 B16 32 DRQ3 R42 10K GND
SA14 33 A17 B17 34 DACK1-
SA13 35 A18 B18 36 DRQ1 R43 10K GND
SA12 37 A19 B19 38 REFRESH-
SA11 39 A20 B20 40 SYSCLK
SA10 41 A21 B21 42 R47 GND
SA9 43 A22 B22 44 IRQ6 10K R48 GND
SA8 45 A23 B23 46 IRQ5 10K R52 GND
SA7 47 A24 B24 48 IRQ4 10K R53 GND
SA6 49 A25 B25 50 IRQ3 10K R54 GND
SA5 51 A26 B26 52 10K
SA4 53 A27 B27 54 TC R55 GND
SA3 55 A28 B28 56 BALE 10K
SA2 57 A29 B29 58 VCC
SA1 59 A30 B30 60 OSC
SA0 61 A31 B31 62 GND
GND 63 A32 B32 64 GND


95.76
90.30
9.02
5.08
I1
J23
J22

🗐 To have a better understanding of network technology

"Network" glossary

ActiveX control

Microsoft Technology that makes the sharing of information between several applications easier. This technology is mainly used to develop interactive applications and the contents of Web sites. The ActiveX controls optimise the OLE technology which has been used for quite some time, by extending the object sharing domain, which was up until now limited to computers, to all the Internet network. The modular design of this technology enables programs which are intended to operate alone to be written, in "intelligent" objects incorporated in other Visual Basic programs or in Web pages, or even into standard OLE objets in documents.

ANSI

The American National Standards Institute is an organisation, which specialises in establishing standards in the United States particularly in the computing and telecommunications fields.

Applet

Computer program written in Java™ language. Applets are identical to applications, with the difference that they do not operate alone. Moreover, they follow a set of conventions with which they can be executed in a Java compatible browser.

ARP

This is the acronym for Address Resolution Protocol, which allows a machine in the network to associate an IP address to a hardware address.

ARPAnet

ARPA is the acronym for Advanced Research Project Agency, for the minister of Defence in the United States. This is the source of the creation of computer networks over wide areas. The ARPAnet network was the forerunner of Internet.

Authentication

Electronic signature. This technology is used to guarantee the authenticity of the source of an electronic transmission.

BBS

Bulletin Board System: message and information server that can be accessed with a microcomputer equipped with a modem.

Baud

Data transmission speed of a modem or other device. This unit of speed measures, on a technical level, the number of events or signal changes per second. (the term "baud rate" is commonly and incorrectly used to designate the number of bits per second, which is a different unit of measure).

Browser

Client program used to search for networks, extract and display copies of files in a simplified reading format. The current standard browsers can also use associated programs to execute sound and video files. Mosaïc, Netscape Communicator, Microsoft® Internet Explorer are the most widely used browsers.

CERN

Conseil Européen pour la Recherche Nucléaire, the European Laboratory for Particle Physics located in Geneva, Switzerland, where at the end of the 1980s a team of engineers, lead by Timothy Berners-Lee, created the World Wide Web technology.

CGI

Acronym for Common Gateway Interface, software which makes the communication between a Web server and programs running off this server easier; for example, programs which process interactive forms or which search for information in databases on the server, following a request from a user.

The IP2 system incorporates a CGI interface allowing the execution of commands from the interpreter. With the IP2 system's CGI interface, the interactions with the inputs and outputs of the IP2 equipment can be performed from a simple web browser.

Clients

Client programs giving access to network resources by processing the information on a server (see below). For example, a browser is a client.

Contents

Combination of text, images, sound files, data or any other information presented by a Web site.

Continuous transmission of an audio file

Sound files captured in real time in an audio file or transmitted in real time over Internet. A plug-in added to the Web browser decompresses and reads the data as it arrives on the computer. The continuous transmission of an audio or video file eliminates the waiting time which results from downloading all the file and thus allows the entire file to be read with a help program.

Cookie

File stored on the hard disk of a computer, used to identify the computer or the preferences of the user for a remote computer. "Cookies" are often used to identify the visitors of a Web site.

DATAGRAMME

A datagramme is a discrete packet of data which contains the addresses, and which is the basic transmission unit on an IP network. It can also be called a `packet'.

DLCI

DLCI means `Data Link Connection Identifier, it is used to identify a unique point to point virtual link via a Frame Relay network. DLCIs are normally assigned by the frame relay network provider.

DNS

Domain Name Service: Service which attributes the names of the sites / addresses on Internet according to a naming plan. In France, the national domain .fr is managed by the INRIA.

Domain

The part of an Internet symbolic address which identifies an organisation that is a member of the network and which specifies the level of this organisation in the Internet network.
(ex. : ulb.ac.be which signifies: Université Libre de Bruxelles (Brussels Open University), academic, Belgium)

Domain name

On Internet, the name of a computer or group of computers used to identify its electronic (and sometimes geographic) location for data transmission. The domain name generally contains the name of an organisation and is always followed by a suffix of two or three letters that designate the type of organisation or the country of the domain. For example, in the domain name Microsoft.com, Microsoft is the name of the organisation and com is the abbreviation of commercial. Therefore this is a commercial organisation.

The following suffixes are also used in the United States: gov (government), edu (educational institution), org (organisation, generally non-profit-making), and net (general; may or may not be commercial). Outside the United States, a two-letter suffix indicates the country of the domain, for example uk (United Kingdom), de (Germany), and jp (Japan).

Download:

Action of transferring a file stored on a remote computer.

Downloading

Procedure aiming to request and transfer a file from a remote computer to a local computer, then to save this file on a local computer. This procedure is generally carried out via a modem or a network.

Email or Electronic mail

Method that allows the transfer of written messages between different stations on a computer network. The two most frequently used electronic mail software programs are Microsoft Exchange and Eudora.

Encoding

Scrambling process for transmitted information. The encoding can be used to cleverly filter data to hide it from being understood by third parties. This process exists in two different forms: software encoding, easy to install and the most widely used, or electronic chip encoding which is more difficult to install, but faster and above all, more difficult to decode.

Ethernet

Local network using a coaxial cable and bus topology. The data transmission speed is normally 10Mbps.

Eudora

Software (PC / Mac) which controls the composition, sending and reception of electronic mail on Internet.

FAQ

Acronym of frequently asked questions, list of questions and answers available for users on, for example, a particular technology or software. It is recommended reading the FAQ list before calling or sending a message requesting technical assistance, as the answer to your question may be written there.

AZTEC RADIOMEDIA updates and publishes a FAQ per product family on its Web site. Internet address: http://www.aztec.fr/support/faq.htm

Firewall

Software designed to prohibit any unauthorised access into a computer network.

Frames

The frames technique divides the window which is used as a WWW browser to display an HTML document in several windows where it is possible to present HTML documents that are independent of one another.
See HTML.

Freeware

Software where the royalties are not protected. This type of software is often found on Internet. It must be distinguished from the voluntary contribution software.
(see below).

FTP

Acronym of File Transfer Protocol, an Internet protocol which allows users to transfer files between computers.

Gateway

System which allows the transfer of information between two networks.

GIF or .gif

Acronym of Graphics Interchange Format, a type of graphic file format designed for World Wide Web documents.

Gopher

Navigation tool on Internet that presents the information in the form of a hierarchical structure of menus - its development was stopped with the arrival of the World Wide Web.

Hardware address

This is the number that identifies, in a unique way, a host on a physical network on the access layer.

Home page

Main page of a Web site. Home pages generally contain links to other locations in the actual site or to external sites. Certain large Web sites can have several homepages.

HTML

Acronym of Hyper Text Mark-up Language. Standardised description language for Web pages. It specifies the formatting of documents using commands (tags, flags, labels) and is

interpreted by the WWW clients such as Netscape, Mosaic or Internet Explorer.
HTML pages are text documents (in ASCII format) which can be made with a text editor or an HTML editor. The principle is basic: the section of text to be formatted is surrounded with flags (tags or even labels); each flag is written between the characters < (less than) and > (greater than) and is interpreted as a command by the browser).

HTTP

Acronym of Hypertext Transfer Protocol, the basic protocol of the World Wide Web technology. HTTP represents a set of instructions for the software, which controls the transmission of the HTML documents on Internet.

Hypertext, HTML

Acronym of Hypertext Mark-up Language. Electronic text in a format which procures an instantaneous access, via links, to another hypertext in the same or another document.

Hypertext link

Reference or link, in the form of a specifically encoded text or graphic image, connecting a given point in an HTML document to another point in the document or another document on the World Wide Web, or even to a particular point in another document on the Web. When you click on a hypertext link, it sends you to the point or document designated by the link.

IETF

Internet Engineering Task Force. Committee which works on the standardisation of transfers on Internet.

Internet

In its largest sense, an internet network is a large computer network made up of a certain number of smaller networks. Internet with a capital "I" refers to the physical network which makes up the Web and which has enabled the electronic mail to reach a world-wide level.

Intranet

Private network inside an organisation. The Intranet networks often use the Internet protocols to deliver their contents. They are often protected from the Internet network by firewalls.

IP address

Internet protocol address of a computer connected to Internet, normally represented by 4 numbers separated with decimal points, for example 128.121.4.5

ISDN (RNIS)

Acronym of Integrated services digital network, a network that acts as a digital connection service for the telephone and communication devices. An ISDN connection can procure an Internet access at a relatively high speed (up to 128.000 bits per second).

ISP

Acronym of Internet service provider, an Internet access provider for companies and private individuals, via ISP servers.

Java™

Object orientated programming language developed by Sun Microsystems, designed for the creation of applets or programs which can be applied to Web documents. It is possible to insert an applet in an HTML page, in the same way as an image. You display a page containing a Java applet using a browser, which handles the Java language. The applet code is then transferred to your system and executed by the browser.
Of course, the IP2 equipment Web server supports Java applets.

. .JPG or JPEG

Acronym of Joint Photographic Experts Group, a type of graphic file format designed for Web documents.

LAN

Acronym of Local Area Network, a network that connects two or more computers in a relatively limited area, often within an organisation, to exchange and share files.

Link

Abbreviation for hypertext link. A link refers to a reactive zone in a Web document. It is normally distinguished from the rest of the text by a different colour. It is possible to click on a link to open an object coming from the active or other database, another document, an HTML page on the Web or a local Intranet.

MAC address

This is the hardware address in the case of Ethernet networks

MIME

Multipurpose Internet Mail Extensions. Designates a set of extensions for the routing of electronic mail allowing elements other than text - such as graphics, sounds or faxes.

Modem

Acronym of modulator/demodulator, hardware that connects a computer to other computers or to Internet, via a standard or ISDN telephone line (see below). A modem can be internal, integrated in a computer, or external. An external modem is a unit that connects the computer to a telephone line. The various modems are distinguished by their data transmission speed, expressed in baud (see above). At present, the standard modems operate at 28.800 or 33.600 baud and the most recent models reach speeds of about 56.000 baud.

MSS

The Maximum Segment Size (MSS) is the largest quantity of data that can be transmitted at a time. If you want to avoid fragmentation, MSS must be equal to the MTU-IP header. MSS does not need to be set on IP2 equipment.

MTU

The Maximum Transmission Unit (MTU) is a parameter that determines the longest datagramme that can be transmitted by an IP interface without needing to be split into smaller units. The MTU must be larger than the largest datagramme that you want to transmit without being split up.

Note: this only provides local protection from fragmentation, other links on the route can have a smaller MTU and the datagrammes will be split up in this place. Typical values are 1500 bytes for an Ethernet interface, or 576 bytes for a SLIP interface.

Multimedia

Term designating any contents which combine text, graphics, sound and/or video files.

NCSA

Acronym for the National Centre for Supercomputing Applications, advanced research centre in Illinois University in Urban-Champaign, where the scientists and engineers have developed the largest part of the technology on which the World Wide Web is based. Mosaic, the first browser capable of displaying graphics, was developed by the NCSA.

Net

The term Net, with a capital "N", is an abbreviation of Internet.

News

Messages that supply the discussion groups of the Usenet network.

Newsgroup

Discussion group that is part of the Usenet network and which treats a particular subject.

NIC

Network Information Centre: service responsible for the authority and management of naming plans. A NIC service exists for every country in the world that works in co-ordination. In France, the management of the naming plan .fr is done by INRIA by delegation from the NIC.

NNTP

Network News Transfer Protocol. Protocol used to transfer the news on Internet. See news, newsgroup, usenet.

On-line service

Subscription to a paying service to make access to Internet easier. This type of service proposes, for example, information or financial bulletins presented in a structured way. Amongst the main on-line services, there is America Online (AOL), CompuServe and MSN, Microsoft Network.

Packet

See DATAGRAMME

Password

Code that the user must type during an access procedure to certain computer systems.

Platform

System hardware and software on which a computer system is based.

Plug-in

Component or software module which improves the capacities of an application, generally to be able to read or display files of a certain type. For the Web browser, the plug-ins are used to display rich contents such as audio, video files or animations.

POP

Post Office Protocol. Protocol used for the recovery of electronic mail stored on a server by means of client software.

PPP

Acronym of Point-to-Point Protocol, a connection configuration of computers via a telephone line or a network link acting as a telephone line.

Protocol

Set of rules or standards established for the communication of data on a network, in particular Internet. The computers and networks communicate via protocols that determine their mutual behaviour so that the transfer of information can be carried out.

Real time

The real time that a task needs to be carried out. The information is processed with an immediate response time and without any time delay.

Script or script language

Programming shortcut which enables users with little technical experience to create a rich content on their computer which offers programmers a fast means of creating simple applications.

Search engine

Program or service used to locate files on an Intranet or on the Web. The access to a search engine is generally done using a browser such as Microsoft Internet Explorer. Some of the most well known search engines are Excite, Yahoo!, WebCrawler, Infoseek and Lycos. New search engines are permanently being developed.

Server

Computer, or its software, which "serves" other computers on a network by managing the files and the operation of the network. The computers "served" by a server integrate client software (see above). The Microsoft Internet Explorer browser is an example of client software.

Signature

Electronic mail or Usenet function which indicates the author of the message and/or the origin of it. The signatures can communicate your mood of the moment or the thought of the day. A signature can transmit a quantity of information, at the end of a message, but by courtesy, it is preferable to limit it to a few lines.

Signet

Computing procedure that allows the user to record a network site so as to be able to easily return to it. By clicking on a signet, the user accesses the desired site directly without having to pass by the normal connection path. A collection of signets is called a signet list.

Site

Set of related Web pages, residing on the same server and interconnected by hypertext links.

SLIP

Acronym of Serial Line Interface Protocol, a type of switched protocol used to connect a computer to Internet.

SMTP

Acronym of Simple Mail Transfer Protocol. Protocol used to send and transfer electronic mail.

SPAM

Electronic posting of diverse and varied information, most of the time of an advertising nature and generally sent in bulk to uninterested recipients.

String

Set of alphanumeric characters used as data to be processed to perform calculations or searches.

Surf

Slang for "browsing on Internet". Signifies navigation without a specific purpose rather than for a targeted search.

TCP / IP

Combination of acronyms for Transmission Control Protocol and Internet Protocol, both are protocols that administer the way in which computers and networks control the flow of information on Internet.

Telnet

Terminal emulation program which allows a user to connect to another computer, in particular a mainframe computer such as those on which catalogues of on-line libraries are installed. When a user connects to one of these catalogues of electronic libraries, via Telnet, he obtains access to the files containing the recordings.

Terminal emulation

Technique that allows the remote use of a central computer by making it think that the work is being done on a terminal which is locally connected to it. Telnet is the protocol defining the terminal emulation on Internet.

Uploading

Procedure aiming to transfer a file from a local computer to a remote computer, via a modem or a network.

URL

Acronym of Uniform Resource Locator, the address which specifies the electronic location of an Internet resource (a file). An URL address is generally made up of four parts: the protocol, the server (or domain), the path and the filename, although in certain cases, the path or the filename is not included.

Usenet

Data communication information service on which the readers can exchange information, ideas, advice and opinions.

VRML

Acronym of Virtual Reality Modelling Language, a set of codes used to write files designed for three-dimensional virtual reality programs.

W3 Consortium

Industrial consortium managed by the Laboratory for Computer Science of the Massachusetts Institute of Technology in Cambridge. W3 is the abbreviation of World Wide Web. This consortium favours the development of standards and encourages the inter-operation between the World Wide Web products. To begin with, based at the European Laboratory for Particle Physics (CERN) in Geneva, Switzerland, where the World Wide Web technology was developed, the Consortium has not totally succeeded its venture which aimed to stimulate the co-operation concerning Web technologies amongst a certain number of private groups, often not very inclined to supply their secrets.

Web

Abbreviation of World Wide Web.

Webmaster

Site administrator. Person responsible for a World Wide Web site.

Whois

Program that can be used to interrogate directories in order to obtain information on a user. (ex: his electronic address).

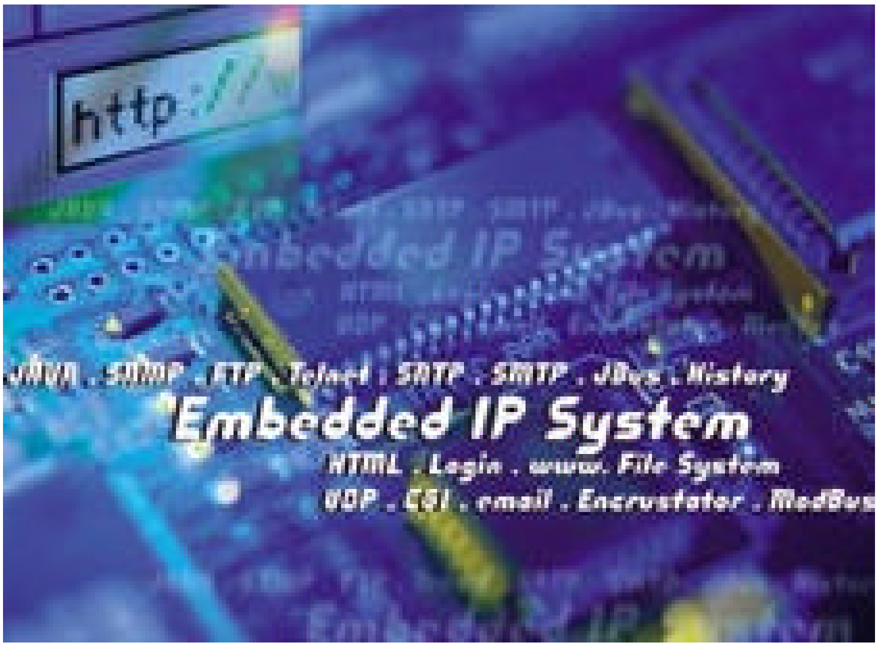
World Wide Web

Collection of multimedia contents interconnected by links and which offer a user-friendly, graphic interface to browse on Internet.

For all information on the IP2 system and the range of equipment IP2com , IP2switch,...

Consult:

www.aztec.fr


http://
JAVA . SNMP . FTP . Telnet . SNTP . SMTP . JBus . History
Embedded IP System
HTML . Login . www. File System
UDP . CGI . email . Encrustator . ModBus

AZTEC RADIOMEDIA
Electronics acting via networks